ENHANCING ACCESS TO JUSTICE IN AUSTRALIAN COURTS USING WEB 2.0 APPLICATIONS

Jennifer K Farrell
BA (UNSW) LLM (UNSW)

June 2017

Macquarie Law School
Macquarie University

This thesis is submitted in fulfilment of the requirements for the degree of Doctor of Philosophy at Macquarie University

Enhancing Access to Justice in Australian Courts Using Web 2.0 Applications

ABSTRACT

Digital access to justice is concerned with the provision of access to justice by courts using the innovative and disruptive technologies of Web 2.0, such as online social networks and virtual courts. While the use of such a digital pathway by the courts is relatively new, analysis at an early stage offers the opportunity to assess the extent to which such innovative technologies should be used in an online environment which is characterised by a heightened tension between access and privacy.

The term, access to justice, generally can be applied to diverse legal concepts and remains for many an idealistic aspiration, one that is difficult to assess as a quantifiable concept, although recognised as a fundamental human right and an essential component of the rule of law. Digital access to justice is provided by innovative and disruptive technologies which have been seen to provide the solution to legal inefficiencies, although they have the capacity to facilitate the misuse of information and inadvertent disclosure of personal data.

In such a context, a critical question is to what extent the innovative technologies of Web 2.0 should be used to enhance access to justice in the digital age. This is a normative question to which I have applied a framework of theoretical and empirical analysis, particularly qualitative analysis. The theoretical analysis of access to justice and the protection of privacy have placed technologies, such as online social networks and virtual courts, within the context of the current regulatory framework to determine to what extent change will be necessary. The empirical analysis has applied mixed methodologies of case studies to analyse the use of Twitter by the Supreme Court of Victoria and the use of a questionnaire to analyse eCourtroom by the Federal Court and the Federal Circuit Court of Australia, providing insight into the problems faced by courts in the use of Web 2.0 applications. While both quantitative and qualitative analysis have been used, the emphasis in my empirical research has been on qualitative analysis to provide the depth and detail required to answer the normative question, relying on mixed methodology to provide the validity and reliability required.

This research fills a gap in the literature on the way in which Australian courts are engaging with innovative technologies to enhance access to justice. It has found that the limitations and boundaries on the use of new technologies have been set substantially by regulatory prudence on the part of the courts and the tension between providing both access and the protection of personal data. This tension can be resolved by recognition of the radical transformation in the information environment, by a reconceptualisation of privacy and by a change of focus from the incremental ex ante legal protection of privacy laws to a consideration of issues such as the 'right to be forgotten' and those more fundamental to the digital age.

I have concluded that, although the use of Web 2.0 applications by Australian courts is currently limited, they have the capacity to enhance access to justice by providing efficiencies, cost savings and improved communication. It is an expectation in the digital era that the use of such applications is synonymous with open justice and direct dialogue with the community. I have recommended more comprehensive strategies to facilitate the extended use of Web 2.0 applications in the future to ensure that access and openness is achieved as well as the protection of personal data. This will require a proactive consideration by policy makers of the future role for the rule of law in a society faced with rule by technology.

Statement of Candidate

I certify that the work in this thesis entitled 'Enhancing Access to Justice in Australian Courts Using Web 2.0 Applications' has not previously been submitted for a degree nor has it been submitted as part of requirements for a degree to any other university or institution other than Macquarie University.

I also certify that this thesis is an original piece of research and it has been written by me. Any help and assistance that I have received in my research work and the preparation of the thesis itself have been properly acknowledged.

In addition, I certify that all information and literature used are indicated in the thesis.

The research presented in this thesis was approved by the Human Research Ethics Committee No **5201400688** on 28 July 2014.

…….
Jennifer K Farrell (42308321)

Acknowledgements

This thesis is dedicated to
Dr Christopher Richard Farrell
(1945-2000)

I would like to express my gratitude to my Supervisor Associate Professor Niloufer Selvadurai for her support, guidance and encouragement, to Professor Islam for his assistance when it was most needed and to Professor David Weisbrot who was so instrumental in the early stages of this journey.

I am most grateful to Warwick Soden, Chief Executive Officer and Principal Registrar of the Federal Court of Australia, who has provided inspiration and leadership in technology for Australian Courts. I also wish to thank the judges of the Federal Court of Australia, especially Justice Robertson, Justice Moore and the late Justice Hill for their encouragement, as well as the Deputy District Registrars who so willingly participated in my empirical research. For the encouragement and assistance from a very special former associate of the Federal Court, Selena Bateman, I give my heartfelt appreciation and gratitude.

Most importantly, I would like to thank my friends and family, particularly Emily, Carl and Peter for their loyalty and love.

Table of Contents

Abbreviations

AAPs	Australian Privacy Principles
ALRC	Australian Law Reform Commission
APEC	Asia-Pacific Economic Cooperation
A2J	Access to Justice Author
CC	Creative Commons (for copyright licence)
CCPIO	Conference of Court Public Information Officers
DDR	Deputy District Registrar
DHS	Department of Homeland Security
ECHR	European Court of Human Rights
EFF	Electronic Frontier Foundation
EU	European Union
GDPR	General Data Protection Regulation
OAIC	Office of the Australian Information Commissioner
OECD	Organisation for Economic Co-operation and Development
OSN	Online Social Networks
PACER	Public Access to Court Electronic Records
PET	Privacy Enhancing Technology
TCP/IP	Transmission Control Protocol/Internet Protocol – the language used by a computer to access the internet
TET	Transparency Enhancing Technology
UK	United Kingdom
US	United States of America

Chapter One: Framing access to justice in a disruptive regulative environment

1.1 Introduction

The innovative developments of Web 2.0 have demonstrated considerable potential to enhance access to justice by transforming communications and provide a digital pathway. The question is whether they should be used by Australian courts and, if so, to what extent. Paradoxically, the openness made possible by these digital innovations has challenged the concept of open courts and privacy, increasing the tension between the free flow of information online and the protection of personal data. The challenge for Australian courts in using Web 2.0 applications is to ensure that these innovative technologies serve the courts' paramount objective of preserving the rule of law and the administration of justice, thus ensuring that the loss of privacy is not the cost of digital access in the future. The objective of this thesis is to consider the tension between digital access and the protection of personal data in the digital era and to recommend changes that enable Web 2.0 application to enhance access to justice while preserving privacy.

Digital access to justice will be defined within the framework of the concept 'access to justice' as it has developed since the 1970s. Innovative technologies have the capacity to transform access to justice in the digital era. Web 2.0 applications have changed the nature of access to courts and moved justice to an interactive[1] arena creating a complex regulatory environment[2]. While these innovative technologies have the capacity to provide more openness for courts and improve access to justice, few have questioned the value of expanded access to justice. The prodigious disclosure of personal data has been viewed more as the price of access than as an inherent danger.[3] The term, access to justice, itself has been viewed as a 'political, legal

[1] The term 'interactive' in relation to computers and applications refers to applications and software that accepts input from humans in the form of data or commands. They provide more personal connection by receiving data and creating modifications. Interactive applications can be created using programs such as Maple 15 <http://www.maplesoft.com>.

[2] This regulatory environment has also been described as a matrix, a term used in a multitude of contexts, including computers, mathematics, social networks, anatomy, printing and geology. It is used by Roger Brownsword to explain the ethical reasoning about technology in the context of bioethics and articulate how to frame the limits of regulation. In *Rights, Regulation and the Technological Revolution* (Oxford University Press, 2008), 32, Roger Brownsword describes a bioethical triangle and three-cornered matrix that impacts on how we choose to frame the limits of regulation. It is a useful metaphor to provide an understanding of the network of regulation and flow between elements in the regulatory environment.

[3] Lawrence M Friedman, 'Access to Justice: Social and Historical Context' in Vol 11 *Access to Justice*, Mauro Cappelletti and John Weisner eds, (Giuffee, 1978) 6-36, 33.

and rhetorical symbol of undeniable power and attractiveness', one that is 'evocative and double-edged' calling for legal change while reaffirming law and legal procedure.[4]

In this chapter, I will examine the literature relating to the regulation and control of disruptive applications, particularly the transformative nature of more recent digital access which has impacted on the role of law and technological regulation. Innovative technologies have raised a dilemma for law by providing more open access to justice, improved communication and efficiencies while at the same time raising extensive and unforeseen problems relating to the protection of personal data. I will also provide an overview of the historical development of Web 2.0 applications and their innovative developments some of which have been supportive, in that they sustain the current paradigm, and innovations that are disruptive in transforming the current regulatory paradigms and have transformed our understanding of concepts such as privacy.

As the adoption of such applications by the courts can be considered to be in the initial stages of implementation, it is a relevant time to consider their development and impact. I will first explore the nature of Web 2.0 and its use as a platform for increasing access to justice, distinguishing 'sustaining technologies' and 'disruptive'[5] technologies using the terms 'sustaining' and 'disruptive' as useful categories in a legal context to explain the current innovations. In addressing these challenges I will apply a theoretical analysis and use empirical data on innovative technologies used by courts, exploring, as well, the regulatory policies suggested in the literature and the changes that may be required to effectively manage digital access.

[4] Austin Sarat, 'Book Review' (1981) 94 *Harvard Law Review* 1911-1924, 1911. In this book review Sarat considers Mauro Cappelletti et al *Access to Justice* Vol I and Vol II.

[5] Clayton Christensen, *The Innovator's Dilemma* (Harvard Business Review, 1997). The terms 'disruptive' and 'sustaining' innovative technologies originated in the work of Professor Clayton Christensen and his work on disruptive technologies and the innovator's dilemma. This theory was developed in the context of business management, however, they are useful categories for innovative technologies of Web 2.0 as applied in law. The term 'sustaining technologies' refers to new technologies that foster improved performance of established products, although they may be 'discontinuous or radical in character'. Most innovation falls into this category, 13-14. The term 'disruptive technologies' refers to technologies that perform differently, often underperforming established products but are typically 'cheaper, simpler, and frequently, more convenient to use'. In a business context, Christensen viewed them as 'vexatious phenomena for good managers to confront successfully',16, and proposed a practical framework to enable managers to understand the role of disruptive technologies.

1.2 Background

1.2.1 The innovative developments of Web 2.0

The internet in the 21st century has made 'an unprecedented proliferation of self-expression' possible.[6] It has been recognised as 'one of the most powerful instruments of the 21st century for increasing transparency in the conduct of the powerful, access to information, and for facilitating active citizen participation in building democratic societies.'[7] Quantities of data unimaginable even 30 years ago have been placed online by government agencies, private corporations and individuals. This personal data has been collected, aggregated and in many cases linked to create digital profiles. Online personal information now has a permanency and accessibility not previously thought possible. The plethora of information now available on the internet and the distinguishing features of Web 2.0 are transforming access to justice in innovative and unexplored ways, providing a communication platform with collaborative applications.

The more recent developments in innovative applications[8] have provided improved communication but also created problems relating to law and regulation by the extraordinary growth of user-generated content. The innovative applications of Web 2.0[9] have challenged the idea that control over human behaviour and information on the internet is achievable. It has led to the perception of an online 'Wild West'[10] where 'modern technology is totally out of control'.[11] Such technology has also raised significant issues relating to the extent that security is possible for personal data, particularly the capacity of government agencies to protect it.[12]

---

[6] Jonathan Barrett and Luke Strongman, 'The Internet, the Law, and Privacy in New Zealand: Dignity with Liberty?' (2012) 6 *International Journal of Communication* 127-143, 128.

[7] Frank La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,* Report to the Human Rights Council, 17th session, UN Doc A/HRC/17/27 (2011) <www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf> 4.

[8] These include: wikis or collaborative websites where anyone can contribute and edit. Some are limited to particular communities. They can be general or specific and include images, sound recordings or videos; blogs or web logs which provide information or comments on a particular issue, usually maintained by a small group or an individual and usually allowing comments by visitors to the site; online social networks include organisations such as Facebook and Twitter.

[9] Susan Butler (ed), *Macquarie Dictionary* (Macquarie Dictionary Publishers Pty Ltd, 6th ed, 2013). Web 2.0 is defined as: 'a perceived altered state of the World Wide Web, equivalent to a second generation of a software product, which features social networks, creative commons, wikis and other such sites that encourage user input and information sharing' 1669.

[10] Carlisle George and Jackie Scerri, 'Web 2.0 and User-Generated Content: legal challenges in the new frontier' (2007) 2 *Journal of Information, Law & Technology* (now renamed *European Journal of Law and Technology*) 2 <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2007_2/george_scerri>.

[11] Owen Bowcott, 'Superinjunctions: Modern technology out of control, says lord chief justice' *theguardian* (online) 20 May 2011. The Lord Chief Justice of England and Wales, warned that action should be taken against

The term 'Web 2.0' appeared in an article by DiNucci[13] in 1999 where the web of the future was seen as one 'identified only by its underlying DNA structure-TCP/IP (the protocol that controls how files are transported across the Internet) … the ether through which interactivity happens'.[14] The first discussion of Web 2.0 as a concept can be found in O'Reilly's analysis in a conference in 2005.[15] Davis referred to Web 2.0 as an 'attitude not a technology'.[16] He considered that what was important about Web 2.0 was not the applications themselves but 'participation, openness and communication'. He also considered the semantic web, sometimes referred to as Web 3.0, a part of Web 2.0. O'Reilly later expanded on this concept referring to discussions about Web 3.0 and beyond as missing the point because the term was not like a software release number but a '"smarter" system' issuing in a new era where 'the Web is now the world'.[17]

Subsequent to O'Reilly's article there has been considerable discussion[18] about what the concept means but, as O'Reilly has explained, it does not have a 'hard boundary, but rather, a gravitational core'. By this he means that Web 2.0 is a set of principles and practices. He considered that there was 'something qualitatively different'[19] about Web 2.0 which is why the term has endured. The contrast between Web 1.0 and Web 2.0 was discussed in its application to the business world as the difference between the internet of Web 1.0 being used

people who defy court injunctions and publish lies on social media and websites. <https://www.theguardian.com/law/2011/may/20/superinjunction-modern-technology-lord-judge>.

[12] Judith Ireland, 'Refugees could win status over breach', *Sydney Morning Herald* (Sydney) 20 February 2014, 7. This article reported the in advertent disclosure of details of thousands of asylum seekers on the Immigration Department's website. The matter was investigated by the Privacy Commissioner and the Immigration Department.

[13] Darcy DiNucci, 'Fragmented Future' (1999) 32 *Design & New Media* 220-222.

[14] Ibid 220.

[15] Tim O'Reilly, 'What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software' (2007) 65 *Communications & Strategies* 17-37, 17.

[16] Ian Davis, 'Talis, Web 2.0 and All That', *Internet Alchemy* (4 July 2005) <http://blog.iandavis.com/2005/07/talis-web-2-0-and-all-that/.

[17] Tim O'Reilly and John Battelle, 'Web Squared: Web 2.0 Five Years On' (2009) Web 2.0 Summit <http://web2summit.com>.

[18] Jonathan Strickland, 'How Web 2.0 Works' (2007) *Tech* <http://computer.howstuffworks.com/web-204.htm/printable>. In this article Strickland attributed the term to Dale, Dougherty, O'Reilly Media publisher. He presents a summary of the main debate and the lack of consensus about the meaning of the term (8-11). Tim Berners-Lee, the inventor of the World Wide Web, was described a dismissing the concept of Web 2.0 as 'jargon', not describing anything new. Authors such as Russell Shaw were reported as referring to the term as a 'marketing slogan' with conflicting goals and broad concepts. Paul Graham was seen at first as dismissing the concept as a buzz word but later recognized that it referred to the best way of using the web with high levels of interactivity and connectivity. Andrew Keen was reported as considered it merely 'digital narcissism' because so much information was being loaded onto the internet that no one reads it.

[19] Tim O'Reilly, 'Not 2.0?' (5 August 2005) *Radar*: *Insight, Analysis and Research about Emerging Technologies* <http://radar.oreilly.com/2005/08/not-20.html>.

'to provide isolated information silos' and of Web 2.0 being used 'creatively, as a platform to foster innovation'.[20] It is not software with different versions but an integrated suite of services, using the platform of the internet[21] to deliver software as a continually updated service and one which redefines the way users interact, an approach to using the internet creatively to provide flexibility and efficiency. This can be distinguished from the pre-1990s Web 1.0 era which has been described as 'a benignly anarchic and anomic space for freedom of expression that, in principle and practice, should be liberated from established legal traditions and social pressures'.[22] Nevertheless, Web 1.0 provided the opportunity for courts to publish judgments[23] on their websites and provide accurate information about the legal system and the courts to meet the challenge of maintaining public confidence in the judiciary.[24]

The salient characteristics of Web 2.0 can be found in the seven principles O'Reilly identified. These were: first, the use of the web as a platform; secondly, he described it as 'harnessing collective intelligence' by the use of an 'architecture of participation' where users add value by the use of applications such as web blogs (internet opinion postings); thirdly, 'database management' became the core competency of Web 2.0 companies rather than software management which emphasised the importance of data; fourthly, the change from updated software releases to a system of continual updating of software; fifthly, innovation and

[20] IBM Corporation, *The business value of Web 2.0 technology: IBM's vision for tapping the collective knowledge of the extended value chain* (Report, September 2007)
<ftp://ftp.software.ibm.com/pub/lotusweb/web20/10709800_Web_2.0_brochure.pdf> 3.

[21] The technology being used is Asynchronous JavaScript and XML or AJAX which uses existing standards but allows a server to update a web page without reloading the whole page and is faster. Also application programming interfaces or APIs is software that is used to allow Web 2.0 applications to integrate with other applications or improve functionality.

[22] Barrett and Strongman, above n 6, 127.

[23] From 1995 the Federal Court of Australia judgments were published in Hyper Text Markup Language (HTML) to enable them to be published on a webpage. An archive of judgment summaries is available on the Federal Court website <http://www.fedcourt.gov.au>. Until 2012 most judgments were published on AustLII <http://www.austlii.edu.au> and could be obtained from a link on the Federal Court website. On 3 August 1999 the Federal Court became the first Australian Court to broadcast live streaming video and audio of a judgment summary over the internet in *Australian Olympic Committee Inc v Big Fights Inc* (1999) 46 IPR 53. Links to the judgment and summary, video and video transcript of matters of public interest such as the decision in *Wik Peoples v State of Queensland* [2004] FCA 1306 and *Seven Network Limited v News Limited* [2007] FCA 1062 are also available from the Federal Court website. Anne Fitzgerald et al, 'Open Access to Judgments: Creative Commons Licences and the Australian Courts' (2012) 19 *Murdoch University Law Review* 1-52, 26 proposed that a copyright-based management strategy should be adopted which would facilitate access to judgments, use and dissemination in digital form. These authors considered that the Creative Commons (CC) would allow use of the judgments in accordance with Web 2.0 capabilities while 'ensuring their integrity and accuracy'.

[24] Chief Justice M E J Black, 'New Technology Developments in the Courts – Usages, Trends and Recent Developments in Australia' (Paper presented at the Seventh Worldwide Common Law Judiciary Conference, May 2007) 4.

'lightweight programming models' using the Creative Commons (CC) licence[25] with some rights reserved and which create value by the assembly of components in an innovative way; sixthly, the use of multiple devices, and finally, the provision of an enriched user experiences.[26]

With the web as a platform, the role of software changed to being one used to deliver services and manage data. Open source software gained a new level of importance, particularly with the use of CC licences which made innovation and re-use common. This reflected a different mindset, encouraging innovation and the creation of value by assembling components of the software in innovative ways. The web platform became almost invisible and more useful for different devices such as phones and handheld devices as well as personal computers. The innovation and flexibility in the platform enable integrated communications and 'rich user interfaces' allowing the 'wisdom of the crowds' to improve and influence the development of Web 2.0.[27]

There was no reliance on web browsers and web servers but a system that delivered services over the web platform, illustrated by the difference between Netscape's[28] reliance on 'the old software paradigm' and Google[29] which 'began its life as a native web application', a 'specialized database' where the 'value of the software is proportional to the scale and dynamism of the data it helps to manage'. One of the most significant characteristics of Web 2.0 is the development of a new role for applications, that of data management, and the provision of 'software as service' which connects the edges of the internet. The potential for wider distribution of information has been referred to by Anderson[30] as reaching 'the long tail', not just the centre of the internet but the outer limits, improving distribution of information and diversity. The change in the role of software from one of a product to a service, the use of open source software with users as co-developers led to data management as the essence of the software working seamlessly as an 'almost invisible part of their

[25] Creative Commons provides tools that provides flexibility in the use of software by allowing individuals and companies to keep their copyright and allow certain uses of their work under a relatively flexible licence which can often only be limited by the requirement of acknowledgment <http://creativecommons.org>.
[26] O'Reilly, above n 15.
[27] Ibid.
[28] Netscape was known for Netscape Navigator its web browser <http://www.netscape.com>.
[29] Google was founded as a search engine and later added other products such as electronic mail (Gmail) <http://www.google.com>.
[30] Chris Anderson *The Long Tail: Why the Future of Business is Selling Less of More* (Hyperion Books, 2008). In this book Anderson explains the new business model in the internet age where online businesses can reach the previously untapped markets or 'tail markets'.

infrastructure' and an 'innovation in assembly' where value is created by assembling services in new ways. This also allows 'perpetual experimentalism'[31] and flexibility.

The O'Reilly principles are related and can be summarised into two seminal characteristics: first, the internet as a platform for the delivery of services and for communication; secondly, the collaborative interaction made possible by this platform. These seminal characteristics[32] – the web as a platform and collaborative interaction - can be applied to the digital pathway to justice[33] in the Web 2.0 environment to assist in analysing the distinctive features of the online changes where a qualitatively different system of justice delivery can be provided.

The first characteristic, the web as platform, is demonstrated by the functionality of the Commonwealth Courts Portal.[34] This is described on the website as an evolving system that provides information about cases in the Federal Court, the Family Court of Australia and the Federal Circuit Court of Australia and contains a selection of information from the formal record of the courts. The Portal provides access to web-based services and selected information about cases before the courts. It also provides a Federal Law search[35] of selected information for the Federal Court or Federal Circuit Court. There is a Live Chat facility which allows users to chat online with an agent from the Family Court about questions relating to procedural issues and to an agent in the Federal Circuit Court about efiling

[31] Ibid.

[32] Andrew Chadwick, 'Web 2.0: New Challenges for the Study of E-Democracy in an Era of Informational Exuberance' (2008) 5 *I/S: A Journal of Law and Policy* 9-41. (Reprinted in S Coleman & P M Shane (eds) *Connecting Democracy Online Consultation and the Flow of Political Communication* (MIT Press, 2012) 45-75). The seminal characteristics of Web 2.0 have also been applied to a study of eDemocracy by Chadwick. Chadwick referred to the quantitative and qualitative shifts in the online environment and used O'Reilly's principles to analyse the broader implications for political behaviour. Chadwick discussed the use of the internet as a platform for political discourse; the use of collective intelligence; the importance of data and the "controversies surrounding privacy, surveillance and the commercial and political use of personal information"; the perpetual experimentalism in the public domain and the collaboration; the creation of small scale forms of political engagement through consumerism and the propagation of political content across multiple applications, and the rich user experience available on political websites, particularly the use of online videos on sites such as YouTube. Chadwick concluded that there was 'real value in online consultation and public policymaking' despite its difference to the 'deliberative public sphere'.

[33] I am using the term digital pathway in this dissertation to refer to all the electronic applications, processes and technologies used in the legal system including: electronic files, electronic filing, electronic courtrooms and all applications based on the court websites, including the portals <http://www.comcourts.gov.au>.

[34] The Commonwealth Courts portal is an integrated electronic interface providing links to websites and applications. This portal links to the Federal Court of Australia, the Family Court of Australia and the Federal Circuit Court.

[35] The details Federal Law Search has a database which is updated in real time and includes all cases commenced since 1 January 1984. It also includes information such as the name of participants, file number, date commenced and type of application or appeal. It does not include the contents of filed documents. This is only available on inspection of documents in the Registries and subject to the rules of the courts <https://www.comcourts.gove.au/pas/fed_esearch>.

information. Access to the eCourtroom[36] is not available through the Portal but through the Federal Court website and it is integrated with eLodgment.[37] These factors emphasise the value of data.

There are now an extensive array of legal websites online which are used for the delivery of information and services in many countries.[38] Staudt considered such websites as vital 'foundational building blocks for transformational delivery changes' providing an '[i]nternet framework on which to hang new services and new approaches to collaboration. Their authenticity and interface consistency' making them viable platforms for delivering information and innovation.[39]

The second group of characteristic of Web 2.0 relates to the 'collective intelligence' which has been made possible by the 'architecture of participation' and interaction to be found in web blogs and particularly in online social networks (OSNs) which invite input of personal data for participation and which encourage disclosure and the sharing of personal information. The architecture of participation in relation to Australian courts will be discussed in more detail in chapters Four and Five of this thesis.

Wolf[40] has proposed collaborative technology[41] as a way of improving support for pro bono programs and providing 'cost effective ways' for unrepresented litigants 'to overcome the inherent disadvantages associated with lack of counsel' and so improve access to justice.[42] Wolf focussed on the needs of unrepresented litigants which he found were increasing in number, including not just '[l]ow income Americans' but also 'increasing numbers of those

[36] <https://www.ecourtroom.fedcourt.gov.au/ecourtroom/default.aspx>

[37] Details about eLodgment can be found on the Federal Court of Australia website. It is a web based service to electronically file documents in Federal Court and Federal Circuit Court of Australia proceedings without the need to attend Registry, saving time and costs. It is available for use by practitioners, law firms, corporate bodies or self-represented litigants but not for third parties. It is a service available at any time of the day, although documents eLodged outside normal registry hours (after 4.30 pm) are processed during normal business hours <http://www.fedcourt.gov.au/online-services/elodgment/faq-started>

[38] An example of the type of services made possible by this technology is to be found in the United States where low income people have been targeted for assistance with the Technology Initiative Grants program which has provided a national network of legal aid websites, provided access to document preparation programs, allowed people to apply for assistance at any time through the internet, assisted military members, veterans and their families with legal assistance through StatesideLegal (<http://www.StatesideLegal.org>) and provided an online system for low income people to claim tax credits.

[39] Ronald W Staudt, 'All the Wild Possibilities: Technology that Attacks Barriers to Access to Justice' (2009) 42 *Loyola of Los Angeles Law Review* 1117-1145, 1126.

[40] Michael J Wolf, 'Collaborative Technology Improves Access to Justice" (2012) 15 *New York University Journal of Legislation and Public Policy* 759-789.

[41] Ibid 762. Wolf refers to interactive technology via the Internet as 'collaborative technology'.

[42] Ibid 788.

with moderate incomes'. He saw the use of collaborative technology as offsetting unmet legal needs, allowing resolution of disputes in ways other than litigation; as useful in reducing 'legal knowledge deficit' when interacting with the court system; and making traditional legal and alternative dispute resolution services 'more accessible and affordable by lowering transaction costs and increasing efficiency'.[43] He referred to the recommendations of the Senior Counselor for Access to Justice, US Department of Justice, who considered an improvement in access to justice would be achieved by developing infrastructure so unrepresented litigants could use web-based legal assistance and government services; encourage electronic form assembly and efiling systems to assist these people to 'diagnose their legal problems'; promote technology literacy and the widespread utilization of videoconferencing technology.

Wolf used the specific examples of online document assembly service, such as 'ready-to-file court documents', to assist unrepresented litigants with a lack of procedural expertise.[44] A second example used by Wolf was the use of unbundled legal services which may take many forms, including a lawyer providing limited representation in court and the client and lawyer collaboratively preparing legal documents or in other cases using online services such as Rocket Lawyer.[45] The third suggestion was the creative adaptation of 'familiar online technology' such as video conferencing for lawyers to provide services online; allowing appearance by lawyers remotely; and the use of videos to provide legal information.

Technologies such as A2J Author[46] can potentially introduce transformational changes in access to justice.[47] They can provide such tools as: public access to document assembly; internet-mediated 'customer friendly' direct services to clients; service delivery using 'deep integration'[48] of systems via the internet and greater co-ordination of systems; as well as direct internet connection between legal aid case and document management systems and agencies

[43] Ibid 772.

[44] Ibid 779.

[45] Ibid 784. Wolf discussed the assistance provided to self-represented litigants by the use of collaborative tools online at Rocket Lawyer. Clients are provided with step-by-step instructions on customizing and completing documents, access to lawyers to review the work, ask legal questions and discounts for legal services when these are necessary <http://www.rocketlawyer.com>.

[46] Access to Justice Author (A2J Author) is a cloud based software tool that delivers greater access for self-represented litigants enabling web-based interfaces for document assembly to be built. These take complex legal information from legal forms and present it to self-represented litigants in a way that the forms can be easily completed and prepared for filing in the courts. It is a service available free to courts, legal services organizations and other non-profits for non-commercial use. Over 1.8 million documents have been assembled using this system since 2005: <http://www.a2jauthor.org>.

[47] Staudt, above n 39.

[48] Ibid 1128. This refers to the integration and interface of legal aid agencies' internal document and case management systems with customer-facing systems.

and courts. Staudt refers to A2J Author as 'the thin veneer-making tool' which assists effective communication with the public.[49]

Both characteristics of Web 2.0 applications provide new opportunities for accessing legal information and innovative procedure with an almost limitless capacity for openness and instant access. It is one of the most dynamic and attractive qualities of Web 2.0. Some of the inherent characteristics of these applications including openness, collaboration and innovation are consistent with basic legal principles and have opened up new possibilities for access to government, politics and law, providing through Web 2.0 principles, a digital pathway to justice. The digital pathway to justice made possible by Web 2.0 applications is an evolving and, at times, controversial one, particularly the possibility of providing unlimited data disclosure, however it is 'an achievable and increasingly implemented reality'.[50]

1.2.2 Web 2.0: a platform for innovation and 'disruption'

Christensen's analysis of sustaining and disruptive technologies[51] has been considered relevant to sectors other than business, 'for assessing the impact of innovation across sections where technological change manifests itself in similar ways, including financial consulting, emerging markets, media, education, health care, and the legal market'.[52] It is a useful framework for analysing innovative technologies used in courts.

The strength of Christensen's theory is in the clarity and depth of his explanation of both 'sustaining technologies' and 'disruptive technologies' and their conflicting demands. His methodology and conceptual analysis about the problems of managing disruptive technological change have been applied to media, education, health care and legal markets,

[49] Ibid 1145.
[50] Luciano Floridi, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality* (2014, Oxford University Press) 162.
[51] Clayton Christensen presented a theory of disruptive innovation which he saw as creating a new market which would disrupt existing markets and replace products: Clayton Christensen *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail* (Harvard Business Review Press, 1997). The theory was first presented in 1995 in an article by Joseph L. Bower & Clayton M. Christensen, 'Disruptive Technologies: Catching the Wave' (1995) *Harvard Business* Review 45. Christensen in an interview in 2011 with Joan Richardson, 'Disrupting How and Where We Learn' 92 *Phi Delta Kappan* 32 (<http://www.jstor.org>) explained disruptive innovation as "an innovation that transforms the complicated, expensive services and products into things that are so simple and affordable that you can I can use them". He considered his theory to be generically applicable.
[52] Raymond H. Brescia et al, 'Embracing Disruption: How Technological Change in the Delivery of Legal Services can Improve Access to Justice' (2014) 78 *Albany Law Review* 553-621, 556.

although not without some criticism. Lepore[53] considered it no more than a theory about why businesses fail, not a 'law of nature' and an idea that is 'blind to continuity' and a 'very poor prophet'. Her criticism is centred on what she sees as a distinguishing feature of non-industrial ventures which do not sell commodities for gain and have 'obligations that lie outside the realm of earnings', such as the obligation of a doctor to a patient. This is a valid criticism in the application of such a paradigm to law and the courts where a consideration of the administration of justice is paramount. Nevertheless, the terms are useful for analysis and in assisting an understanding of the types of innovation.

In applying this theory to the legal profession, Brescia et al, recognised the 'monumental, transformative shift in shape and focus' due to technologies which have 'commodified' legal services, making them less expensive and more accessible.[54] These transformative changes were recognized by Susskind who identified disruptive developments in technology such as automated document assembly, online dispute resolution, 'relentless connectivity', online legal services, automation and enhanced project management.[55]

The use of the term 'disruptive innovation' has more recently been seen as one that has 'gone from theory, to buzz word',[56] generalised to refer to the 'monumental, transformative shift in shape and focus that will change the practice of law forever'.[57] Brescia et al concluded that access to justice could be improved in the US by embracing 'some aspects of the current and upcoming disruptions to the profession' which would happen at the margins, where people are underserved and priced out of the market.[58] Their concerns about such disruption were whether the application of technology would be a substitute for an 'individual receiving full representation by an attorney that is tailored to his or her needs … '; a substitute for 'that constellation of services, benefits, accountability, and oversight'; whether the quality of the information and guidance would be good enough or better than nothing; and that such services would 'divert funds from full-service representation'.[59]

[53] Jill Lepore, 'The Disruption Machine: What the gospel of innovation gets wrong' (June 23, 2014) *The New Yorker* <http://www.newyorker.com/magazine/2014/06/23/the-disruption-machine>.
[54] Brescia et al, above n 52, 553. These authors acknowledged the provision of legal services by non-lawyers as a somewhat controversial part of the transformation with some claiming that there will be fewer lawyers required and others criticizing the quality of legal services provided.
[55] Richard E Susskind, *The End of Lawyers? Rethinking the Nature of Legal Services* (Oxford University Press, 2008)
[56] Neal Katyal, 'Introduction: Disruptive Technologies and the Law' (2014) 102 *Georgetown Law Journal* 1685-1689.
[57] Brescia et al, above n 52, 553.
[58] Ibid 611-612.
[59] Ibid 553.

Other authors, such as Sourdin have adapted the Christensen analysis to the specific legal context of dispute resolution. In assessing the role of emerging technologies in the 'continuing evolution of judicial processes and the justice system in general',[60] Sourdin identified three main categories: the first 'supportive technology'[61] which support 'an understanding of and engagement in the justice system', referring to legal information and applications that improve services, as well as Facebook and other OSNs; secondly, 'replacement technologies'[62] which 'replace certain interactive parts of justice processes', such as online dispute resolution which replaces face-to-face conferences with video conference; and thirdly, 'disruptive technology' which 'may significantly change ADR and judicial processes', referring in this category to Artificial Legal Intelligence and computer systems that perform tasks without requiring human intelligence.[63]

Many innovative technologies can be seen as replacement technologies and in general terms, disruptive. As Christensen has found, most innovative technologies are supportive and sustain the current paradigm. It is what he refers to as the 'disruptive' technologies that can be transformative. In a legal context, they have the potential to challenge current regulatory paradigms and our understanding of concepts such as privacy, forcing a re-evaluation of online regulation.

The challenge for law and policy makers in this field is to implement innovative development in technology, using Web 2.0 as a platform for innovation, in a way that enhances transparency and access to justice while protecting privacy.

1.3 Nature of the research

1.3.1 The research question

The primary question to be addressed is:

> *To what extent should the innovative technologies of Web 2.0 be used to enhance access to justice in the digital era?*

[60] Tania Sourdin, 'Justice and technological innovation' (2015) 25 *Journal of Judicial Administration* 96-105, 96.
[61] Ibid 97.
[62] Ibid 98.
[63] Ibid 101.

The question is aimed at examining access to justice in the age of rapid technological development and the challenging issues created by the use of disruptive applications, exploring the extent to which Web 2.0 applications can be used by the courts. Brownsword has argued that the framework for the use of technologies, determining what 'can be licensed, what cannot be entertained, and how far we can go',[64] can be found in moral concepts such as privacy which he considers remain important boundary markers for determining questions of the legitimacy of the use of technology.[65] He identified privacy as a 'central element of ethical reasoning about technology'.[66]

The extent to which regulations can provide an environment for innovative technologies to enhance access and protect privacy can be related to the regulability of the internet. It was considered in the early days of the internet that it was unregulable, however, Web 2.0 has been shown to present a complex regulatory environment which is highly regulable and where non-compliance can be designed out by code and algorithms, limiting a role for the rule of law. Koops has suggested that data protection and privacy have been highlighted as in need of much more than the current legal protection and an area where possibly '[c]ode as law' can supplement these laws. Such embedded legal rules in 'present and future ubiquitous technologies' such as transparency enhancing technologies (TETs) and privacy enhancing technologies (PETs), providing a 'socio-technical infrastructure' to protect weak parties.[67] Brownsword has recognised that there will need to be a role for the rule of law and technological regulation in the future where the 'normative regulatory environments will co-exist and co-evolve with technologically managed environments'[68]. He has warned that a regulatory environment needs to allow the normative values of law to flourish.

One of the objectives of this research is to offer insights into possible regulatory solutions to ensure Web 2.0 applications can be used to enhance access to justice and resolve the tension between open justice and privacy. Its significance is in recommending policy and legal changes which will provide a more flexible regulatory environment. This thesis will contribute to the substantial literature on access to justice and privacy in the field of digital access and the implementation of Web 2.0 applications by the courts.

[64] Roger Brownsword and Morag Goodwin, *Law and the Technologies of the Twenty-First Century* (Cambridge University Press, 2012) Brownsword, 188.
[65] Ibid, Chapter 8, 188-224 and Chapter 9, 225-245.
[66] Ibid 223.
[67] Bert-Jaap Koops, 'Law, Technology, and Shifting Power Relations' (2010) 25 *Berkeley Technology Law Journal* 973-1036, 1029.
[68] Roger Brownsword, *Rights, Regulation, and the Technologies Revolution* (Oxford University Press, 2008) 14.

1.3.2. – Issues to be addressed

The main issues to be addressed in determining the extent to which Web 2.0 applications should be used to enhance access to justice include the following:

1. The first issue to be examined is the nature of access to justice in the era of digital communication. Web 2.0 applications promise to deliver almost limitless transparency and open justice, thereby enhancing the nature of the access to justice. The issue is whether such applications have transformed our understanding of the concept since its analysis in the 1970s.

2. The second issue concerns the immediacy and transparency of Web 2.0 applications and whether the practical obscurity of the past has been transformed into overexposure. This openness relates not only to the virtual courts and online court documents but to OSNs such as Twitter and Facebook. The increased pressure to disclose information, not only within OSNs but also in the context of virtual courts and electronic court documents, has blurred the boundary between public information and private information. Web 2.0 applications appear at first glance to provide the openness that has been recognised as facilitating the principle of open courts, however, access to justice and privacy have been viewed as concepts in conflict, essentially contested.[69]

3. Privacy and the protection of personal data relating to the use of Web 2.0 applications in the digital era is the third issue to be considered. For some, privacy is an anachronism, unattainable in an interactive world. Others consider privacy is an essential element in protecting human dignity. The limitations and boundaries for

[69] The idea of a contested concept was discussed by W B Gallie, 'Essentially Contested Concepts' (1956) 56 *the Aristotelian Society* 167-198. Gallie proposed four conditions for a finding of essential contestedness: they must be appraisive; the valued achievement that the concept signifies must be internally complex; there is nothing absurd in any one of a number of possible rival descriptions of its total worth; and the accredited achievement must admit considerable modification in the light of changing circumstances. The examples he refers to are: art, democracy, social justice and religion. Human dignity has been presented as better understood as an essentially contested concept because Rodriguez considered it assisted in explain the theoretical disagreements about the concept and its place in the international legal regime: Philippe-Andre Rodriguez, 'Human dignity as an essentially contested concept' (2015) *Cambridge Review of International Affairs* <http://dx.doi.org/10.1080/09557571.2015.1021297>. In contrast it has been argued by Kenneth M Ehrenberg that law should not be considered an essentially contested concept because it does not assist in illuminating the most general concept of law, however, it was conceded that it would be more appropriate to apply this term to the rule of law.

technologies that promise to enhance access to justice will be imposed by the extent to which privacy can be accommodated in an open and accessible world.

4. As specific Web 2.0 applications provide different levels of protection for personal data and different access, the fourth issue to be considered is whether general principles relating to the provision of digital access and the protection of privacy can be derived from research into the use of specific Web 2.0 applications: the use of Twitter by the Supreme Court of Victoria and the use of a virtual court by the Federal Circuit Court and the Federal Court of Australia. Will continual evaluation and modification of Web 2.0 applications be a necessary part of their implementation?

5. The final issue concerns a determination of the limits that should be placed on Web 2.0 applications, particularly disruptive technologies by the courts. This raises issues of regulatory control in a complex online environment where disclosure of personal data is ubiquitous. The regulatory environment for online technologies is neither static nor predictable but constantly adapting to the fast moving developments in technologies, providing new forms of communication and interaction across 'temporal and geographical distances'.[70] They are spaces which have developed new norms of regulation and redress and where 'public ordering' has been challenged by 'private ordering' and self-designed alternatives.[71] The changes have led to concerns about the legitimacy and effectiveness of regulations, particularly in relation to the protection of personal information in such an open and accessible environment. Regulatory consensus has not yet been achieved, in part due to the differing underlying understanding of what privacy means and how it can be protected in the face of interactive technological change. The legislative changes to privacy law alone have not provided the required level of protection. The issue of redefining privacy is one that will be explored to determine whether the EU understanding of the concept provides more protection in the digital era.

This thesis argues that exploitation of personal data need not become a cost of enhancing access to justice by the use of Web 2.0 applications and that the tension between access and

[70] Lawrence Friedman, 'Digital Communications Technology and New Possibilities for Private Ordering' (2003) 9 *Roger Williams University Law Review* 57-69, 64.
[71] Ibid 57-69.

privacy can be resolved within the complex regulatory framework by reconceptualising privacy and the application of a philosophy of information.

1.4 Literature review: regulation and control of disruptive applications

1.4.1 Introduction

The literature review in this chapter will be confined to the regulatory environment and the role of law in setting boundaries for the use of disruptive innovations. Further analysis of the literature relating to 'access to justice' and 'privacy' will be considered in greater detail in Chapters Two and Three respectively, due to the extensive nature of the research in those areas. The literature discussed in this section will set the context for the research question and the theoretical framework for understanding the extent to which innovative technologies of Web 2.0 can be used to enhance access to justice.

The technological changes ushered in by Web 2.0 have demanded a regulatory response, one that law has been seen as slow to provide.[72] The introduction of interactive technologies has been incremental and the development of adequate regulation piecemeal, in no small part due to the complexities of regulation in the online world. This online world is global in nature challenging the traditional national jurisdictions more characteristic of law.[73]

However, the regulation of new technologies offers a great deal to 'engage the interest and attention of all who claim to be lawyers, sociologists and philosophers and express an interest in the health of the rule of law'.[74] As Brownsword has predicted by 2061 there will be a 'pervasive use of 'technological management' in place of traditional legal rules'[75] with the domain of law 'set to shrink'.[76] This change could challenge fundamental philosophical and ethical principles, disrupting the regulatory environment and it highlights the need for a philosophical framework.

[72] Michael F Fleming and Christina L Kunz, 'Foreword: Riding The Long Wave of Developing Law', (2011) 37 *William Mitchell Law Review* 1666-1670, 1669.
[73] Michael Kirby, 'New Frontier: Regulating Technology by Law and "Code"', (2007) 18 *Australian Intellectual Property Journal* 230-345, 237.
[74] Ibid 240.
[75] Roger Brownsword, 'In the year 2061: from law to technological management' (2015) 7 *Law, Innovation and Technology* 1-51, 2. In this article Brownsword has taken the year 2061 as significant as it represents 100 years after the publication of HLA Hart's *The Concept of Law* (Clarendon Press, 1961; 2nd ed 1994). Brownsword asserts that Hart's rule model will by then be totally out of touch with the use of modern technologies as regulatory instruments.
[76] Ibid 4.

1.4.2 The disruptive nature of the regulatory environment and its threat to privacy

The early myth of the independence of cyberspace and 'Barlow's dream of digitally-enabled, stateless cosmopolitanism continues to animate projects of democratic renewal two decades later' inspiring Assange's Wikileaks[77] and his effort to 'undermine conspiratorial authoritarian state efforts to control information flows'.[78]

Twenty years ago Barlow[79] declared cyberspace, 'independent' and unregulable, at least by the '[g]overnments of the Industrial World', rejecting current authorities and the questioning the legitimacy of the source of authority. This declaration by Barlow has been referred to as contradictory and in a 'heroic mode of cyber-narrative'.[80] It is representative of a resistance to the introduction of legal control and legislation in the US such as the *Telecommunications Act* (1996) and the *Communications Decency Act* (1996) and their accompanying threat to regulate what was seen as an unregulable space or 'cybernirvana'.[81]

Barlow challenged the legitimacy of the '[g]overnments of the Industrial World' in trying to impose internet regulation, declaring, 'you have no moral right to rule us nor do you possess any methods of enforcement … ' and asserting equality of access in 'creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force, or station of birth'.[82]

[77] Wikileaks was founded by Julian Assange in October 2006 as an international, non-profit organization to publish news leaks and secret information from anonymous sources <http://www.wikileaks.org>.

[78] Daniel Kreiss, 'A vision of and for the Networked World: John Perry Barlow's *A Declaration of the Independence of Cyberspace* at Twenty' in James Barrett and Niki Strange (eds), *Media Independence Working with Freedom or Working for Free?* (Routledge, 2014) 117, 126.

[79] John Perry Barlow, 'A Declaration of the Independence of Cyberspace' (Davos, Switzerland, 8 February, 1996) <https://www.eff.org/cyberspace-independence> .John Perry Barlow is a retired Wyoming cattle rancher (1971-1988), a former lyricist for the Grateful Dead (1971-1995) and co-founder of the Electronic Frontier Foundation (1990). Since May 1998 he has been a Fellow at Harvard Law School's Berkman Center for Internet and Society <https://homes.eff.org/~barlow/m> In a recent interview for *The Economist* (8 February 2016) on the twentieth anniversary of the Declaration, Barlow confirmed his view that 'the governments of the physical world have found it very difficult to impose their will on cyberspace'. He discussed the difficulties that governments experienced in preventing disclosures from people like Julian Assange, Edward Snowden and Chelsea Manning as well as the problems with the prevention of 'bad behavor online'.

[80] Aimee Hope Morrison, 'An impossible future: John Perry Barlow's "Declaration of the Independence of Cyberspace"' (2009) 11 *New Media & Society* 53-71.

[81] J Schofield, 'A Utopia for Thieves' (29 April 2004) *Guardian Online* <http://guardian.co.uk/print/0,3858,4912099-112498,00.html>.

[82] John Perry Barlow, 'A Declaration of the Independence of Cyberspace', <https://www.eff.org/cyberspace-independence>.

In contrast to those who viewed cyberspace as unregulable, Lessig challenged this belief about the internet.[83] He referred to it as contingently regulable, predicting that 'the infrastructure of the Net will become increasingly controlled and regulable through digital identity technologies'.[84] His theory was that as cyberspace[85] is constituted by the code of its software and hardware, there is 'extraordinary potential for control'.[86] According to Lessig's analysis, behaviour on the internet is regulated by law, norms, markets and architecture or code.[87] The code he refers to is the 'application space' which works at the application layer with such systems as browsers, operating systems, encryption, email systems.[88] Code is recognised as resetting the traditional balance between 'freedom and constraint'.[89] In drawing on the work of Mitchell,[90] Lessig predicted an evolutionary future for the internet and recognised the impact of commerce which was making the internet a more regulated space. However, he suggested that there is a choice about the type of code that can be used to govern cyberspace. The limitations on that choice he considered were due to the limits placed on the courts, the limits of the legislature and the limits to our thinking about code.[91] Lessig referred to the early days of the internet and the open and unsecure protocols, designed to be open for research. As the internet changed to support online commerce, so it changed to enable regulation. While it is difficult for governments to regulate behaviour on the internet,[92] Lessig did not consider it was difficult for governments to regulate the architecture of the internet.[93] Architecture is seen as a 'kind of law', determining what people can and cannot do. When controlled by private enterprise, he envisaged that a 'kind of privatized law' is created.[94]

Lessig viewed code writers as 'lawmakers':

[83] Lawrence Lessig, *Code and other Laws of Cyberspace* (1999) Basic Books, New York, 5.

[84] Lawrence Lessig, in the Preface to the second edition (2006) *Code v2* <http://codev2.cc/> x.

[85] Lessig, above n 83, 4 – cyberspace is used by Lessig as a general term to refer to the online 'new society' of the internet. It is not one space but many (63). It has many different 'natures' which are 'given not made' (82). He extends his discussion to the substantive and structural values of online space (7). He considered the regulability of internet and the ability of the government to regulate online behaviour (19).

[86] Lessig, above n 83, 58

[87] Ibid 88-89

[88] Ibid 102

[89] Ibid 142.

[90] William Mitchell is the former Dean of MIT School of Architecture and author of books on the internet such as *Me++: The Cyborg Self and the Networked City* (the MIT Press, 2004).

[91] Lessig, above n 83, 213

[92] Ibid 239. Lessig has borrowed architectural concepts to explain the insights "about the relationship between the built environment and the practices that environment creates".

[93] Lessig, above n 83, 43.

[94] Ibid 59.

> They determine what the defaults of the Internet will be; whether privacy will be protected, the degree to which anonymity will be allowed; the extent to which access will be guaranteed. They are the ones who set its nature. Their decisions, now made in the interstices of how the Net is coded, define what the Net is.
>
> How the code regulates, who the code writers are, and who controls the code writers - these are questions that any practice of justice must focus on in the age of cyberspace. The answers reveal how cyberspace is regulated.[95]

The issue that is raised in this analysis of code writers as 'lawmakers' is a fundamental one concerning the future role for the rule of law. Lessig advocated building into code the capacity to choose with 'machine-to-machine negotiations' which would enable individuals to issue instructions about the informational privacy they wish to protect.[96] It, however, assumes that individuals understand what information they want to protect and the capacity for code to provide this protection.

He was writing at a time shortly after Barlow's declaration. Regulability for Lessig was the 'ability of the government to regulate the behaviour of its citizens … on the Net'[97] where the space is regulated by its architecture and this regulation imposed primarily through code. He used the image of a 'dot' to represent what was regulated and then examined the various constraints that may regulate this dot, the market, law, norms and architecture.[98] The interaction between these modalities and their impact on the regulated were seen as making the internet 'fit the demands of commerce'[99] with architectural changes enabling commerce to gain more control. The questions he posed were whether government should do something to make the architecture consistent with important public values and, if there is conflict with the interests of commerce whether the government should ensure that the public values that are not in commerce's interest should also be built into the architecture.

What was identified by Lessig was that choices of substantive values needed to be made in relation to regulation of cyberspace, for example, whether there will be free speech, or open trade and whether we will have to choose between privacy and access. He considered that the capacity to enable choice must be built into the architecture and code of the internet. His suggestions for future regulations differed depending on the context. In the field of

[95] Ibid 60.
[96] Ibid 163.
[97] Ibid 19.
[98] Ibid 3-8.
[99] Ibid 30.

intellectual property he considered that there should be limitations on control so that a commons is retained, providing an incentive for authors to produce. The tension that Lessig recognised between access and protection in intellectual property and privacy were the same and the choice whether the information should be completely 'propertized' or not was relevant in both field. He recognised the transforming impact of commercialisation of the internet where commercial interests promote strong protection of intellectual property. In contrast, commercial interests were seen as promoting weak privacy protection, although, without protection the incentive to participate in online transactions would be threatened. Law through code was perceived as being able to restore the balance in both areas, making laws stronger to protect privacy and weaker to allow some public access to intellectual property.

Lessig's analysis of four regulatory modalities has been extended by Murray and Scott[100] who demonstrated the 'importance and variety of hybrid forms that real-world control systems take'. They reconceived the four modalities as 'hierarchy, competition, community and design'[101] adding the essential elements of control systems – 'standard-setting, monitoring and behaviour modification". Murray and Scott found Lessig's modalities 'under-inclusive'[102] and considered 'a wide variety of regulatory hybrids' would be useful in developing regulatory control.

The more recent concern raised has been with the degree of 'techno-regulation'[103] and the reliance by regulators on 'non-normative strategies'[104] with the consequent loss of choice and loss of control. The impact of this change being the 'shrinking significance' and questionable conceptual relevance of law in technologically managed regulatory environments.[105] This is also a change which has impacted on the question of legitimacy in the use of these technologies and raised the issue of where the limits or regulatory margins should be placed when the use of technology introduces the danger of designing out non-compliance.[106]

[100] Andrew Murray and Colin Scott 'Controlling the New Media: Hybrid Responses to New Forms of Power' (2002) 65 *Modern Law Review* 491-516.
[101] Ibid 492.
[102] Ibid 501-505.
[103] Roger Brownsword, 'Lost in Translation: Legality, Regulatory Margins, and Technological Management' (2011) 26 *Berkeley Technology Law Journal* 1321-1366, 1322.
[104] Ibid 1343.
[105] Ibid 1324.
[106] Ibid 1323.

Goldsmith and Wu do not consider countries and regions powerless in the face of globalisation and the internet. They addressed the question of whether the impact of the internet on contemporary globalisation will have a lasting effect on nations and government control. While acknowledging the increased difficulties governments have in suppressing communications, they considered the 'physical coercion by government – the hallmark of a traditional legal system – remains far more important than anyone expected'.[107] They found EU laws controversial and aggressive in 'geographic scope' with their privacy laws a 'fourth type of global law'.[108] It may also be that this aggressive stance by the EU on privacy laws is indicative of the need for coercion internationally to provide the necessary protection within EU borders. The longer term impact of the EU stance on privacy laws is a topic for future research.

Technologies, particular new technologies can be highly disruptive,[109] particularly in the context of the 'relative "lawlessness" of the online world'[110] leading to the necessity for 'legal and regulatory oversight'.[111] Brownsword questioned whether regulators could respond to the opportunities offered by new technologies to ensure that 'increments in regulatory effectiveness are not achieved at the cost of a diminution in legitimacy … or, even worse, at the cost of weakening the conditions that are essential for any aspirant moral community to have a meaningful purpose'.[112] A new regulatory environment was seen as being required in the future to answer the challenges of prudence, legitimacy, effectiveness and connection[113] if

[107] Jack Goldsmith and Tim Wu, *Who Controls the Internet: Illusions of a Borderless World* (2006, Oxford University Press), 130. In examining the control of eBay they found that 'below the surface of eBay's self-governing façade revealed a far different story-a story of heavy reliance on the iron fist of coercive governmental power', 132.
[108] Ibid 128 –129.
[109] Disruptive technologies are those that are seen as ones "that will transform life, business and the global economy" – McKinsey Global Institute (May 2013) 'Disruptive technologies: Advances that will transform life, business, and the global economy' <http://www.mckinsey.com> This report indicates that "[l]awmakers and regulators will be challenged to learn how to manage new biological capabilities and protect the rights and privacy of citizens", 1 – this indicates the analysis of new technologies is in the context of economic development, however, the role of new technologies in dramatically changing the status quo can be applied to law as well. Of the twelve potentially economically disruptive technologies mentioned, advances such as in mobile internet, cloud technology and the automation of knowledge work can be identified as relevant to law. The American Bar Association has published a survey report for more than twenty years. The 2014 *ABA TechReport* identified areas such as security, cloud computing, tools for managing legal practice, mobile technology and blogging and social media as areas of interest. An earlier report in 2010 examined Richard E Susskind's suggested disruptive technologies which included: automated document assembly, relentless connectivity and online legal services, as areas of concern in *The End of Lawyers? Rethinking the Nature of Legal Services* (Oxford University Press, 2008).
[110] Brownsword and Goodwin, above n 64 20.
[111] Ibid 22.
[112] Brownsword, above n 68, 28.
[113] Ibid 185-187.

Web 2.0 applications were to be used to provide access to justice without compromising personal data and privacy.

The transition from Web 1.0 to Web 2.0 has been accompanied by a transition in modes of communication and changes in the nature of the disruption. OSNs, for example, while providing new ways of communication, providing faster and more comprehensive communication to another individual or many individuals at the same time, to some extent replacing emails, they also threaten privacy and the security of information. The last ten years, in particular, have seen an increasing concern with the legal problems associated with information technologies and a search for a regulatory solution. Klang[114] examined the way disruptive technology is regulated, examining the 'strong relationship between the regulation of disruptive technology and the Internet-based participatory democracy'.[115] He concluded that it is virtually impossible to use 'legal rules to attempt to control a volatile changeable environment'[116] and the 'regulator must come to accept a certain level of disorder'.[117]

One of the most debated disruptive features of interactive technologies and a challenge for regulation has been the disclosure of personal data and invasion of privacy. This has raised fundamental substantive problems and highlighted a need for regulatory changes. Part of this is due to the 'uncontrollable information spread',[118] the unrestricted user-generated content, speed and accessibility of the internet through a 'myriad of devices'[119] which was seen as creating unique challenges for regulatory schemes in democratic nations, particularly the need to acquire public approval.[120]

A suggested regulatory framework for the management of privacy issues was discussed by Burdon in response to Zittrain's Privacy 2.0 and the development of Web 2.0 applications.[121] Burdon discussed 'geo-mashups'[122] as an example of technological developments of Web 2.0

[114] Mathias Klang, *Disruptive Technology: Effects of Technology Regulation on Democracy*, (PhD), Göteborg University, 2006) <http://hdl.handle.net/2077/9910>.
[115] Ibid ii.
[116] Ibid 39.
[117] Ibid 235.
[118] Renee Keen, '*Untangling the Web: Exploring Internet Regulation Schemes in Western Democracies'* (2011-2012) 13 *San Diego International Law Journal* 351-353, 356.
[119] Ibid 355.
[120] Ibid 380.
[121] Mark Burdon, 'Privacy Invasive Geo-Mashups: Privacy 2.0 and the Limits of First Generation Information Privacy Laws' (2010) 1 *Journal of Law, Technology & Policy* 1-50.
[122] Ibid 2-6. These were defined as 'an information system that combines one or more data streams that is overlaid on an online geographical interface, to create original content.' They are created by using geo-browsers

which have created issues for privacy. These are user generated applications created by aggregating data on an online geographical interface to create original data such as Google Maps.[123] They are illustrative of the salient features of Web 2.0, identified earlier. They use the internet as a platform for the delivery of a service, created by interaction and collaboration, and add value by the use of data which is vital to their existence. One of the difficulties identified by Burdon was the use of personal data which has led to the invasion of privacy by the creation and use of applications such as Spotcrime using Crime Maps which combines data from crime statistics and Google Streetview which have led to the inadvertent disclosure of personal information[124] and Gawker Stalker for celebrity tracking. This collaboration has led to the linking of personal data, whether protected or unprotected, with government or other data available on the internet and invasions of privacy.

Confidence in the security and privacy of information has been found to be vital in ensuring that people would not be deterred from using the justice system. While Zora considered that a different role for courts was necessary in the 21st century[125] with public expectations of accessibility and the use of a 'problem-solving gateway'[126] as well as other technological innovations that facilitate the delivery of services over a distance, and customisation. He envisaged courts as 'access-to-justice institutions' defining 'their role and success in terms of whether they provide access to justice for all'.[127]

> **Technology use may create or magnify conflict between values of openness and personal privacy.** In such circumstances, decision makers must engage in a careful balancing process, considering both values and their underlying purposes, and should maximize beneficial effects while minimizing detrimental effects.[128]
> (emphasis added)

such as Google Maps as a platform to overlay information on mapping interfaces and made possible by application programming interfaces (APIs).

[123] Burdon, above n 122: See also Google Maps <https://maps.google.com.au> In preparing Street View, a component of Google Maps, Google admitted in 2013 that he had collected personal information such as passwords and emails from unencrypted networks as its cars passed by mapping street information. A settlement for $7 million was reached in a case brought by 38 States in the US (David Streitfeld, *The New York Times* (12 March 2013).

[124] Ibid 18.

[125] Richard Zorza, 'Courts in the 21st Century: The Access to Justice Transformation' (2010) 49(1) *The Judges' Journal* 14-19, 34-36.

[126] Ibid 16-17. Zorza considered the gateway system crucial to 21st century justice and a substantial use of technology to enable litigants to choose appropriate pathways to resolve their issues.

[127] Ibid 14.

[128] Ibid 254.

Zorza and Horowitz considered the dual responsibility of the justice system in being open and protecting personal privacy, despite the reality that when there is access there is also 'a significant potential for dissemination of all or part of such information'.[129]

1.4.3 – The role of law in the complex web of regulation

The regulatory environment of the 21st century has been described as a space where there are greater quantities of law and a web of interacting regulatory controls.[130] It is considered that '[r]egulation in the era of global governance has become so extraordinarily complex that no single actor, including states, can hope to manage effectively the processes of modern life'.[131] Law has been presented as forming a significant strand in the complex web of regulatory institutions,[132] something 'that is regulated and that regulates'[133] with courts forming 'distinctive nodes where knots are sometimes tied between difference strands of the web'.[134] Concern has been expressed by a number of authors that the fading of normative signals and the role of law is a particular challenge in technological environments.[135]

In discussing the complex interplay between law and technology and in hoping to provide a 'law and technology theory' which would 'promote more informed policy analysis', Cockfield considered two broad categories of analysis: a liberal approach which would seek legal solutions 'less deferential to legal precedent and traditional doctrine, and a conservative approach, relying more on precedents.[136] The advantages in the liberal approach were seen in its flexibility and 'forward-looking analysis' while a disadvantage would be a certain destabilising of the law by undermining precedent.[137] The conservative approach was considered by Cockfield to create 'greater uncertainty concerning the transformation of the law in comparison to the uncertainty created by the liberal approach'.[138]

[129] Richard Zorza and Donald J Horowitz, 'The Washington State Access to Justice Principles: A Perspective for Justice System Professionals' (2006) 27 *The Justice System Journal* 248-267.
[130] John Braithwaite and Christine Parker, 'Conclusion' in *Regulating Law* (Oxford University Press, 2004) 273.
[131] Brownsword and Goodwin, above n 64, 182.
[132] Ibid 270.
[133] Ibid 289.
[134] Ibid 276.
[135] Arthur Cockfield, 'Towards a Law and Technology Theory' (2004) 30 *Manitoba Law Journal* 383-415; see also Roger Brownsword, 'Lost in Translation: Legality, Regulatory Margins, and Technological Management' (2011) 26 *Berkeley Technology Law Journal* 1321-1366; Ronald Leens and Bert-Jaap Koops, '"Code": Privacy's death or savior?' (2005) *International Review of Law, Computers & Technology* 329; and Mireille Hildebrandt, 'Legal and technological normativity: more (and less) than twin sisters', (2008) 12 *Techné Research in Philosophy and Technology* 169-183.
[136] Arthur J Cockfield, 'Towards a Law and Technology Theory' (2004) 30 *Manitoba Law Journal* 383-415, 415.
[137] Ibid.
[138] Ibid 414.

It has been argued, however, because the law has been slow to adapt to technological change,[139] it has been slow to develop procedures to deal with many of the challenges created, leaving other control mechanisms such as markets, norms and architecture to fill the void.[140] The reference to law being slow to adapt has been expressed using the metaphor of the hare and the tortoise with the law the loser in the race to keep up with technological change.[141] This metaphor, Bennett Moses suggested does not express the reality which is more complex as 'most changes to technology fit comfortably within existing legal frameworks'.[142] She identified a number of factors in socio-technical change that impacts on law such as: changes in people's behaviour which may mean that laws do not operate as effectively as they had in the past; with such changes it may not be clear how and to what extent existing legal rules apply; some rules may become obsolete; and, as well, law may be required to shape new developments in technology. What Bennett Moses considered was needed were 'paradigm shifts and regular updates in law'.[143] The best outcome was predicted as emerging from 'collaborative interdisciplinary efforts … across the law-technology border'[144] so that the laws that are framed reflect an understanding of the technology and its uses.

Brownsword and Goodwin analysed the pace of the development of technologies and the regulatory connection between new technologies and current regulation.[145] The nature and reasons for the disconnection that results from technological development were identified as relating to three types of 'mismatch': one between the description of the technology in the regulation the characteristics of the newly constituted technology; between the assumptions underlying the regulation in relation to the uses of the technology in the past and in the present with changing use; and as well the mismatch between the 'presumed business model on which the regulation was predicated' and the actual business model that has developed.[146] The problem with this disconnection was viewed as one creating a situation where: regulatees

[139] Fleming and Kunz, above n 72, 1666. See also an explanation of the law's failure to keep up with technological change by Lyria Bennett Moses, 'Adapting the Law to Technological Change: A Comparison of Common Law and Legislation' 26 *UNSW Law Journal* 394-417.
[140] Lessig, above n 83. The four main modalities of control: law, norms, markets and architecture or code were seen by Lessig as the possible ways that cyberspace can be regulated.
[141] Lyria Bennett Moses, 'Adapting the Law to Technological Change: A Comparison of the Common Law and Legislation' 26 *UNSW Law Journal* 394-417.
[142] Ibid, 766.
[143] Ibid, 772.
[144] Ibid, 786.
[145] Brownsword and Goodwin, above n 64, Chapter 15 and Chapter 16.
[146] Bennett Moses, above n 141, 399.

no longer know where they stand; and where it becomes 'wasteful to expend either legislative or judicial resources' to clarify the regulatory position.[147]

Brownsword and Goodwin do not assume that regulatory disconnection is necessarily a 'bad thing and that, when it happens, every effort should be made to close the gap.'[148] They concluded that the developments should be debated in the interests of regulatory legitimacy and democracy … to determine how the regulatory framework should be adjusted.'[149] This would ensure that a transparent and democratic relationship is maintained between the regulatees and regulators.

The dilemma to be overcome being how new technologies could be adopted in the face of threats to privacy, security and ownership of information. However, these are issues that need to be addressed as technology makes inroads into the legal system and the regulatory environment is threatened by an emphasis on economic/price signals rather than human rights signals and a 'shifting discourse about the role of courts' to a 'user-pays justice'.[150] This has been seen as a 'move to a cost-benefit analysis for potential litigants, so the court's so-called services are only accessed where the benefits outweigh the costs'.[151]

This imposition of 'price signals', as recommended by the Productivity Commission,[152] can impact negatively on access to justice by devaluating the role of courts as 'a fundamental aspect of society'[153] and the third arm of government, dissuading people from participating in the legal system. Technology has played an ambivalent role by emphasising productivity, efficiency and cost savings on the one hand but increasing the burden in other areas of litigation, such as discovery where costs have increased; emphasising improved access to justice and open courts but making privacy protection more difficult on the other hand.

147 Ibid, 419.
148 Ibid.
149 Ibid.
150 T F Bathurst AC, Chief Justice of New South Wales, 'Reformulating reform: courts and the public good' (Paper presented at the opening of the Law Term, Sydney, New South Wales, 4 February 2015, (2015) (Autumn) *Bar News* 32 <www.austlii.edu.au/au/journals/NSWBarAssocNews/2015/13.pdf>.
151 Ibid, Chief Justice Bathurst referred to the Productivity Commission, *Access to Justice* Arrangements (Inquiry Report No 72, 5 September 2014) 558; 'Reformulating reform: courts and the public good' (Paper presented at the opening of the Law Term, Sydney, New South Wales, 4 February 2015, (2015) (Autumn) *Bar News* 32 <www.austlii.edu.au/au/journals/NSWBarAssocNews/2015/13.pdf>.
152 Productivity Commission Inquiry Report, *Access to Justice Arrangements* No 72 (5 September 2014) focused on 'constraining costs and promoting access to justice and equality before the law'.
153 Bathurst, above n 150, 33.

This regulatory environment with decision-making located in central state institutions, international bodies, nongovernment organisations, industry and individuals has been recognised as more diffuse, particularly in relation to internet activities. The regulatory framework of the internet has evolved from a largely unregulated space to one in a constant state of negotiation[154] and flux, in a global environment, in contrast to the traditional, formal hierarchical structure.

Scott found, from an analytic perspective, that it is productive to consider regulation happening in a 'regulatory space'[155] where regulatory regimes interact. The developments in technology, particularly OSNs with their chaotic impact on the regulatory environment have forced a re-evaluation of the limits and potential of law as one of the mechanisms of governance.

Parker and Braithwaite advocated a 'multifocal' regulatory perspective for the analysis of law.[156] This would enable an evaluation of the interactions and a fuller perspective of the law in the digital era, particularly the changes in interaction between legal and non-legal regulation.[157] Regulatory space has also been referred to as an ecosystem, an analogy adopted for understanding digital spaces relevant to online businesses, particularly in relation to interconnected information flows and has added a dimension of the fluctuating and negotiated regulatory space. The concept of digital ecosystems has been used as an appropriate analogy for understanding the digital ecosystems of businesses, particularly the interconnected information flows and how law is modified by social relations and customs. In an analysis of legal regulation Braithwaite and Parker considered the insight that the tools, concepts and

[154] Leonard G Kruger, 'The Future of Internet Governance: Should the U.S. Relinquish Its Authority Over ICAAN?' Congressional Research Service Report, prepared for Members and Committee of the US Congress, 5 May 2015 <http://www.crs.gov> In this report Kruger explains that while the International Corporation for Assigned Names and Numbers (ICANN) does not "control" the Internet the question of how it is governed may set an important precedent in future domestic and international policy debates and is "highly relevant to the broader question of how the Internet should be governed". ICANN is currently the U.S. government, through the Department of Commerce's National Telecommunications and Information Administration (NTIA) retains a degree of authority over the management of ICANN. NTIA and ICANN are joint participants in an Affirmation of Commitments agreement with a separate contract between ICANN and NTIA which authorises ICANN.

[155] Colin Scott, 'Analysing regulatory space: fragmented resources and institutional design' (2001) *Public Law* 1. Scott found that using the metaphor of 'regulatory space' was useful for providing a more useful basis for institutional design and reform. He considered that the concept assisted in explaining the limits and potential for law in a more fragmented environment than the traditional hierarchical structure. Regulatory space was originally described by L Hancher and M Moran, 'Organizing Regulatory Space' in Hancher and Moran (eds) *Capitalism, Culture and Economic* Regulation (1989),.

[156] Braithwaite and Parker, above n 130, 2.

[157] Colin Scott, 'Analysing regulatory space: fragmented resources and institutional design' (2001) *Public Law* 1.

methods of regulatory theory can provide in certain areas of law, as well as how law has been modified by social relations and customs.[158] They also asked how the laws that apply in that space regulate how the law interacts with other 'forms of normative ordering', as well as internally within law. In this online interactive space, privacy was identified as the doctrinal category. The layers of regulation, or 'meta-regulation' form the space for the interaction between private law and public regulation. They concluded that 'effective legal regulation that is not responsive to non-legal normative orderings ultimately fails to accomplish its goals'.[159]

Creating a regulatory environment that enables a 'moral community to flourish' is not a matter Brownsword considered should be treated with indifference, particularly in an era of 'techno-management' where the features of the regulatory environment need to be 'compatible with the ideal of legality'.[160] Privacy itself being seen as the 'central element of ethical reasoning' in the application of technologies.[161]

To achieve a regulatory environment that adequately engages with new technology, four main challenges need to be addressed. These have been identified as prudence, legitimacy, effectiveness and connection.[162] Brownsword refers to the work of Marx[163] who distinguished between two different and incompatible perspectives on the implementation of technology.[164] The first is the view that necessary safeguards need to be implemented to protect the security

[158] Braithwaite and Parker, above n 130, 4.

[159] Braithwaite and Parker, above n 130.

[160] Brownsword and Goodwin, above n 64, 451-452.

[161] Ibid 223.

[162] Ibid 46 - 71. Prudence refers to the "risk-benefit assessment for any new product or procedure" with the judgment of the risks and benefits being based on personal interest; legitimacy concerns procedural legitimacy and whether the right kind of procedures have been adopted before the regulatory position is determined, whether it meets the standards of legitimacy expected and whether the means used to implement the regulatory position are legitimate. The effectiveness depends on whether the regulatory environment achieves the intended regulatory goal and connection whether the regulatory position and procedures adopted are relevant to the developing technologies in the present and in the future.

[163] Gary T Marx, 'Forward', in David Wright et al (eds) *Safeguards in a World of Ambient Intelligence* , Series: The International Library of Ethics, Law and Technology Vol 1 (Springer, 2008) vii, at xiv.

[164] Ibid. Marx's analysis was specifically in the field of ambient intelligence or ubiquitous computing although of importance in its application to information technologies as well. Ambient intelligence (AmI) is a developing field of information systems that has been defined by the Advisory Group to the European Community's Information Society Technology Program (ISTAG) as "the convergence of ubiquitous computing, ubiquitous communication, and interfaces adapting to the user"; "ubiquitous computing refs to "omnipresent computers that serve people in their everyday lives at home and at work, functioning invisibly and unobtrusively in the background and freeing people to a large extent from tedious routine tasks: (Mahesh S Raisinghani et al, 'Ambient Intelligence: Changing Forms of Human-Computer Interaction and their Social Implications' (2004) 4 *Journal of Digital Information.* The terms can also be used more interchangeably, both referring to "the embedding of low visibility, networked sensors within and across ever more environments (called ambient intelligence or Aml in Europe and ubiquitous computing or networked computing in American and Japan: Gary T Marx, 'Forward, in David Wright et al (eds) *Safeguards in a World of Ambient Intelligence* (Springer, 2008) vii.

and privacy of personal information, and to ensure people are treated with dignity. The second is that the implementation should 'maximize the technical potential and interests of those who control the technology'. To resolve the incompatibility, Marx proposes twenty questions framed within a discussion about information technologies which should be asked to ensure that we 'continually encounter and wrestle with unsettling and unsettled issues' to ensure the promises of technology will be delivered. The twenty questions were grouped into the regulatory framework identified by Brownsword, of prudence, legitimacy, effectiveness and connection by Brownsword.

The comprehensive analysis of the regulation and interaction between law and technology by Brownsword and Goodwin placed legal regulation in the more general context of a regulatory environment.[165] They have warned that to give new technologies complete freedom to develop would create certain safety risks and threaten the protection of 'distinctive cultural and social values'.[166] Legal and regulatory oversight were seen an essential element in the application of new technologies, although this would not be unproblematic particularly in protecting fundamental values, such as complex human rights.[167] He saw the challenge for law in the face of developing technologies was one of maintaining continuity and stability, despite technological change; guarding against the dangerous use of technological power; minimising the risks and safeguarding fundamental community values; safeguarding human rights and human dignities, and ensuring that the values of the rule of law are preserved.[168]

The four key regulatory challenges identified by Brownsword and Goodwin were considered essential to enable the regulatory environment to 'support the development, application and exploitation of technologies':[169] first, the assessment of regulatory prudence and precaution so that the precautionary measures are relevant to the risks posed by the technology; secondly, regulatory legitimacy – including procedural legitimacy, legitimacy of purpose and standards and legitimacy of regulatory means; thirdly, regulatory effectiveness, when the interventions taken are 'not fully fit for purpose'; and fourthly, regulatory connection, when the initial

[165] Brownsword and Goodwin, above n 64, 24-45.
[166] Ibid 22.
[167] Ibid.
[168] Ibid 23.
[169] Ibid 46.

regulatory connection has not been made or the regulation has become disconnected and reconnection has failed.[170]

The first, the issue of prudence and precaution is associated with the not uncommon degree of uncertainty of new technologies and the difficulties faced by regulators in face of uncertainty risk.[171] The difficulties regulators face is not only weighing the prospective benefits against the possibly harm but the more complex issue of ethical concerns. In the application of new technologies in providing increased access to justice, this may involve weighing up the benefits of providing more open courts, increased access to information and serving the public interest against the harm of disclosing private data.

In the second element relating to regulatory legitimacy, the concern expressed is, even assuming the authority of the regulators is legitimate, whether there has been inclusive 'public consultation, media debate, parliamentary debate … '[172] It is questioned whether public debate can be meaningful when the 'potential risks and benefits of emerging technologies are far from clear and settled'.[173] This dilemma can be illustrated by the application of emerging technologies in law where the public debate about privacy is changing with the increasing reach of privacy invasive technologies. As Brownsword and Goodwin have pointed out, where there is ethical pluralism and competing ethical views, particular with regard to human rights or human dignity, the way forward for regulators is not so clear.[174] Another related concern identified was the legitimacy of the regulatory means adopted rather than whether the selected instruments will be effective. There may be, for example, concerns that the technologies should not be applied in ways that alter valued practices or invade the 'autonomy or privacy of regulatees'.[175]

Within the third element of regulatory effectiveness, Brownsword and Goodwin recognised a 21st century regulatory dilemma in confronting the 'tension between strategies that are acceptable and strategies that work'.[176] They considered that one of the facts of regulatory life

[170] Ibid 46.
[171] Ibid 47-48.
[172] Ibid 48-49.
[173] Ibid 50.
[174] Ibid 59.
[175] Ibid 60-61. One of the examples discussed is the use of brain imaging in a courtroom to assist in assessing the credibility of witnesses which was seen as challenging the traditional role of the jury and "the golden thread of traditional models of criminal justice that is broken, namely the presumption of innocence".
[176] Ibid 71.

is 'that we simply do not know all the keys to effective regulation'.[177] In assessing regulatory failure, the resources, competence of the regulators and their response can be considered, however the failure may also be due to a disruptive, external factor, such as the global financial crisis or a natural disaster.[178]

The final element, the regulatory connection, is inherent in many new technologies that are constantly evolving. Brownsword and Goodwin distinguished three stages of development because technologies do not arrive fully mature nor arrive into a 'regulatory void': firstly, 'getting connected'; second, 'staying connected' and finally, 'dealing with disconnection'.[179] They concluded that there are no guarantees that the regulatory regime adopted will be effective as it will 'always reflect a tension between the need for flexibility … and the demand for predictability and consistency'.[180]

Brownsword and Goodwin considered that the inherent nature of technological developments and the pace of development have pushed the boundaries of ethical and moral frameworks more than any other human activity. Human rights were seen as 'a relevant point of departure in considering the legitimacy of the content and consequences of technology regulation'.[181] They were suggested as boundary markers in the field of technology regulation because they interact with technology. The first interaction, particularly with new social media, was seen in the clash between freedom of speech and privacy where technology 'played an aggravating role, eroding the ability of courts to enforce decision they have made about the appropriate balance between the two rights, at the same time as technology alters the speed, depth and durability of privacy intrusion'.[182] The second interface was described as more complex where human rights act as regulation, the technological advancement causing the dispute as found in *Evans.*[183] The third interaction described is where technological developments create new

[177] Ibid 61.
[178] Ibid 61-63.
[179] Ibid 63-67.
[180] Ibid 66.
[181] Ibid 225.
[182] Ibid 244.
[183] *Evans v United Kingdom* [GC], no. 6339/05, § 77, ECHR 2007-IV 96, 237-43,246-7. Ms Evans and her partner, J had signed a form, as required by the *Human Fertilisation and Embryology Act 1990* (UK), consenting to IVF treatment. A number of eggs were removed prior to Ms Evans' treatment for ovarian cancer which would render her infertile. Ms Evans had to wait two years after the cancer treatment before the embryo could be implanted. The relationship broke up and J withdrew his consent and requested that the embryos be destroyed. Ms Evans sought an injunction in the High Court requiring J to restore his consent and a declaration of incompatibility under the Human Rights Act 1998 that her rights under Articles 8. 12 and 14 had been breached. Also that the embryos were entitled to protection under Articles 2 and 8. He claims were dismissed on 1 October 2003 (*Evans v Amicus Healthcare Ltd and others* [2003] EWHC 2161 (Fam)) as Wall J considered that J

human rights, such as the right to genetic privacy, the right to internet access and the right to forget, the difficulty arising due to the internal and external indeterminacy of human rights because it was considered that they are unable to overcome 'the incommensurability of ethical disputes'.[184]

Brownsword has questioned how much of law will survive the transition to 'techno-management'. He described the legal approach to regulation as one that included such qualities as 'participation', 'transparency' and 'due process'[185] and saw as vital that 'the processes that lead to the particular techno-regulatory features are compatible with the ideal of legality'.[186] His recommendation was that the regulatory environments that are constructed need to 'enable moral community to flourish, even though the normativity of the foreground signals might have given way to non-normative coding and design'. They considered that a reciprocal engagement and 'comprehensively transparent and democratic relationship between regulators and regulates' needed to be maintained to ensure what is valued about law is not lost.[187]

The development of human rights in the regulation of technology is relatively new. They have been identified by Brownsword and Goodwin as 'boundary markers' in that they determine what technology can be used and developed and the 'outer limit of moral acceptability',[188] although the boundaries may move throughout time and in different cultures. Just as the view of privacy may be different now to what it was two hundred years ago and different in Australia to what is in other countries. Human rights are concepts that are more than simple social norms and can encompass 'fundamental assumptions about human existence'.[189]

could not give unequivocal consent to eh use of the embryos and his consent had been to treatment "together". Ms Evans' appeal to the Court of Appeal was dismissed on 25 June 2004 (*Evans v Amicus Healthcare Ltd.* [2004] EWCA Div 727). The court held that the 1990 Act clearly ensured that the consent of both parties was required. The House of Lords refused leave to appeal. The European Court of Human Rights, sitting as a Grand Chamber, in *Evans v The United Kingdom* found against Ms Evans by a margin of 13 to 4. Her primary claim had been the right to respect for private and family life under Article 8. The Grand Chamber considered whether the legislative provisions as applied in this case "struck a fair balance between the competing public and private interests involved" [76]. It was found that the 1990 Act was "the culmination of an exceptionally detailed examination of the social, ethical and legal implications of developments in the field of human fertilization and embryology, and the fruit of much reflection, consultation and debate" [86]. The four dissenting judges considered that such a sensitive case could not be decided on a "simplistic, mechanical basis" [12] and the legislation had failed to strike the right balance.

[184] Brownsword and Goodwin, above n 64, 245.

[185] Ibid 452.

[186] Ibid.

[187] Ibid.

[188] Ibid 188.

[189] Ibid 189.

Human rights concepts do not always prohibit or permit the adoption of new technology but provide a framework and an understanding of the decision-making process.[190]

Hildebrandt[191] has argued that modern law may need to 'rearticulate its basic tenets into emerging technologies' by developing a new 'generic concept of normativity' which recognises 'the normative force of technologies as well as the normative force of law'.[192] Because technology appears to enforce compliance with rules to a greater extent than previously possible, Hildebrandt identified three questions: the first was whether this was a positive development; the second was how technological developments could be brought under the rule of law due to the changing relationship between law and technology, and finally:

> Will it be possible to re-embody the legal norms that protect us against invasion of our privacy, violation of the presumption of innocence, unfair discrimination *in the emerging technologies they aim to regulate,* while still retaining the underdeterminancy we value as the core of constitutional democracy?[193]

Hildebrandt compared both legal and technological normativity, distinguishing the role of the modern state and the force of both law and technology, including their 'constitutive' and 'regulative' impact.[194] The concerns raised were that in a constitutional democracy democratic consent is necessary for the regulation of society and therefore she considered that technological devices should be brought within the 'regime of democracy and rule of law' when they have a normative impact.[195] Hildebrandt concluded that:

> Thus, the paradox of the 'Rechtsstaat',[196] which implies that the powers of the state can be contested in a court of law that is based on the authority of the state, should be translated into emerging technologies that are used to implement both the

[190] Ibid.

[191] Mireille Hildebrandt, 'Legal and technological normativity: more (and less) than twin sisters', (2008) 12 *Techné Research in Philosophy and Technology* 169-183.

[192] Ibid 179.

[193] Ibid 177.

[194] Ibid 172-175. Hildebrandt acknowledged the work of John R Searle, *The Construction of Social Reality*, (Free Press, 1995). She illustrated his analysis of brute facts and institutional facts e.g. driving a car is a brute fact, as it is not constituted by law, while marriage is an institutional fact, as it cannot exist independent of social interaction". A constitutive rule is one such as the rule that a marriage must be registered. If it isn't registered there is no marriage. A regulative rule is one that regulates existing behaviour, such as driving a car under 100 miles per hour. Violation of the rule doesn't necessarily mean that the person cannot drive a car. Technology is regulative as long as a person can chose the way they want to behave. If, however, it makes it impossible for us not to comply, it is constitutive.

[195] Ibid 179.

[196] Ibid 169. Hildebrandt refers to the 'Rechtsstaat' or 'État de droit' as the Anglo-Saxon equivalent of the 'Rule *of* Law'.

> instrumental and the protective aspects of the law. Thus we may sustain the rule *of* law against the rule *by* law and against a rule *of* technology.[197]

The importance of finding a 'coherent solution' to the challenges offered by technologies was acknowledged by Justice Kirby.[198] He recognised Lessig's thesis that 'code', or the architecture of technological systems, would sometimes incorporate regulatory imperatives into information technology obviating any real choice on the part of the user as to whether or not to conform to the law'[199] and that it added a new dimension that could not be ignored. The incorporation of regulatory provisions in technological codes, Kirby identified as an issue in *Stevens v Sony Kabushiki Kaisha Computer Entertainment.*[200] However, he considered that Lessig's thesis did not cover all current major technologies or the ways law can regulate them.[201] Although, he acknowledged that in the future regulation may not necessarily be by law alone.

Concern about the impact of technological code which could result in individuals losing a sense of moral values was raised by authors such as Kirby, Lessig and Koops.[202] Kirby considered that the scope of technologies analysed will need to be broader and the fields of expertise of participants extended. He found that while case studies of effective and ineffective attempts to regulate technology, nationally and internationally need to be included in the debate, traditional legal analysis and judicial decisions will not provide the final answer to the challenges raised by technologies.[203]

The first time written principles were formulated to govern 'the relationship between technology use, development and innovation, and access to justice' can be found in The Washington State Access to Justice Technology Principles.[204] The Principles identified were:

---

[197] Ibid 179.

[198] Kirby above n 73, 245. The conference at the Centre for the Study of Technology, Ethics and Law in Society (TELOS) was one of the first conferences to address comprehensively the problem of how technologies may be regulated.

[199] Ibid 235.

[200] *Stevens v Sony Kabushiki Computer Entertainment* (2005) 224 CLR 193. This case involved the consideration of "technological protection measures" and "circumvention devices". The issue was whether the appellant sold unauthorised copies of PlayStation games and whether the circumvention device used facilitated circumvention of the technological protection measure – the access restrictions in the Playstation software incorporating the access code stored on an encrypted portion of the CDROM which Sony claimed qualified as a technological protection measure under s 10(1) of the *Copyright Act 1968* (Cth). Justice Kirby considered that the court gave "meaning to innovative legislation designed to respond to new technological developments as they affect copyright law" [199] (1).

[201] Kirby, above n 73, 235.

[202] Ibid 244.

[203] Ibid 245.

[204] Zorza and Horowitz, above n 127, 248.

first, the use of technology by the courts should promote access to justice; second, technology should be used to produce a 'just result' by using a 'just process'; thirdly, the justice system should be open to the public and protect personal privacy; fourthly, the justice system should ensure a 'neutral, accessible, and transparent forums which are compatible with new technologies'; fifthly, public awareness and use should be maximised with the promotion of 'public knowledge and understanding of the tools afforded by technology to access justice'; and finally, best practices should be used to ensure equality of access and fairness. They will be discussed in more detail in the following chapter.

Zorza and Horowitz viewed these Principles as an illustration of the development of an analytical framework for technology, access to justice and the maintenance of values such as openness and privacy.[205] They recognised that openness and privacy need not be in conflict because 'while technology may create opportunities for violations of privacy it also provides ways of protecting it'.[206] This view is in contrast to the 'current public debate, where openness and privacy are seen as competitors'.[207] What they considered needs to be identified are the types of information and the users because personal information, relating to 'personhood' should be given greater protection than information from corporate users.[208] Other factors that were considered of importance were: the possible harm from disclosure; the risk of aggregation of data; the social value of access to the particular information; the danger secrecy can add to the continuation of the wrong; the purposes to which the information will be put and the context of the information. Zorza and Horowitz recommended for example, in relation to the Third Principle, that it should form the basis for detailed rules and sub-principles governing access and privacy, it should be flexible enough to cover a wide variety of circumstance and 'strong enough to protect crucial fundamental values that are often in competition'.[209]

The Access to Justice Technology Principles adopted a broad definition of access to justice and were designed to be the 'governing values and principles' to guide the use of technology.[210] They were given legal force by the Supreme Court of Washington.[211] Zorza

[205] Ibid.
[206] Ibid 255.
[207] Ibid 254.
[208] Ibid 255.
[209] Ibid.
[210] Washington State: Access to Justice Technology Principles adopted by the Washington State Supreme Court, December 3, 2004 by Order No 25600-B, defined 'access to justice' to include the 'meaningful opportunity, directly or through other persons: (1) to assert a claim or defense and to create, enforce, modify, or discharge a

and Horowitz considered that '[o]ne of the most important lessons learned from the development of the Principles was the need for their legitimacy and enforceability'.[212] They were developed following considerable 'consultation, analysis, research, deliberation and negotiation'.[213] They could be considered to be a framework for the management of technology which fits within the guidelines discussed by Brownsword and Goodwin for prudence, legitimacy, effectiveness and connection.[214] The Principles appear to address the concern that with the transformative impact of innovative technologies, 'techno-regulation' can replace legal regulation.[215] This is a change which could diminish the moral commitments of regulation and shift the 'normative' to 'non-normative', creating a regulatory environment 'where non-normative instruments dominate' and we 'seem to be subject to the rule of technology rather than the rule of law'.[216]

It has been considered that unless the 'appropriate prudential risk-minimizing and risk-managing measures' are adopted, developing disruptive technologies will remain 'continently dangerous' with a vulnerability that needs to be addressed.[217] The protection of privacy and personal data online is a concerning area of vulnerability. It has been noted that 'IT and privacy have a hard time passing through the same door'.[218] How then will the courts in providing openness and transparency through digital access to justice, also facilitate privacy or at the very least provide a 'minimum and non-negotiable level of privacy protection'?[219] Koops has warned of the dangers for access to justice that technology presents, particularly as 'inequality compensation in legal domains is challenged by technology'.[220] The 'inequality

legal obligation in any forum; (2) to acquire the procedural or other information necessary (a) to assert a claim or defense, or (b) to create, enforce, modify, or discharge an obligation in any forum, or (c) to otherwise improve the likelihood of a just results; (3) to participate in the conduct of proceedings as witness or juror; and (4) to acquire information about the activities of courts or other dispute resolution bodies.' Access to justice was also considered to require a 'just process' with 'timeliness and affordability' and 'transparency' <http://www.courts.wa.gov> .

[211] See <http://www.courts.wa.gov>.

[212] Zorza and Horowitz above n 127, 265.

[213] Ibid 248 and 263.

[214] Brownsword and Goodwin, above n 64.

[215] Hildebrandt, above n 180; see also Mireille Hildebrandt and Bert-Jaap Koops, 'The Challenges of Ambient Law and Legal Protection in the Profiling Era' (2010) 73 *Modern Law Review* 428-460.

[216] Brownsword, above n 103, 1361.

[217] Roger Brownsword, 'The shaping of our on-line worlds: getting the regulatory environment right' (2012) 20 *International Journal of Law and Information Technology* 249, 255-256.

[218] Ronald Leenes and Bert-Jaap Koops, '"Code": Privacy's death or savior?' (2005) *International Review of Law, Computers & Technology* 329, 338.

[219] Ibid 339. Leens and Koops refer to a conclusion of the Working Party on the Protection of Individual with Regard to the Processing of Personal Data, Opinion 1/98, Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS), 16 June 1998.

[220] Koops, above n 67, 974.

compensation'[221] he viewed as the 'key legal mechanism to regulate power relations'[222] by providing rights to the weaker parties to rein in the dominant power of the strong, and of particular relevance in areas such as access to justice. He calls for 'adaptation to meet the new reality'[223] and new forms of legal protection to maintain a 'reasonable balance of power'.[224] It is technology that is seen as challenging the traditional balance of unequal power relationships.

Technologies such as Web 2.0 applications, present 'a more destructive violation of privacy'[225] than has been faced in the administration of justice in the past. New methods for 'accessing, searching, gathering, integrating, analysing, organizing, evaluation, using, and disseminating information'[226] are now possible, such that even the use of the 'generally benign word "access" may give the false impression that the privacy violation ends at the point of access'.[227] As well, the global implications of the legal changes that are needed to facilitate the development of a sustainable policy in the future add to the complexity.

The highly disruptive nature of the regulatory environment has been viewed as challenging the role of law in regulation. The weakness of this regulatory environment is evident in an analysis of the invasion of privacy caused by innovative applications such as OSNs.[228] Web 2.0 is dominated by commercial applications, open communication and control by market forces. For law, the drive for efficiencies and open communication has questioned the security and protection for personal data. The goal will be to achieve, as Brownsword has suggested, a regulatory environment where a 'moral community'[229] is valued and can develop,

[221] Ibid 977. This legal phenomenon is described by Koops as being "based on the idea that in society there are specific parties that have a structural, systematic advantage over other specific parties".
[222] Ibid 974.
[223] Ibid 1027.
[224] Ibid 994.
[225] Zorza and Horowitz, above n 129, 254.
[226] Ibid.
[227] Ibid.
[228] See detailed discussion of OSNs in Chapter Four of this thesis, 'Online social networks: enhancing or diminishing access to justice?'
[229] Brownsword and Goodwin, above n 64, 184-185: Goodwin refers to the three-cornered matrix that Brownsword considered dictates the form in which ethical reasoning about technology takes place. It consists of three essential forms; the first, goal-orientated; the second, rights-based; and the third duty-based. These forms are related to the main normative frameworks of application in technology regulation, particularly in the western world which were considered by Brownsword to be: utilitarianism (the first of the matrix, goal-orientated); deontology (the second, duty based) and liberalism (the third).

one which is compatible with the 'ideals legality and the rule of law'[230] and where normativity is not lost in translation.[231]

1.5 – Methodology

My research question is a normative question. It sets a normative framework within which empirical observation; particularly qualitative analysis can be used to support the normative argument. A combination of doctrinal and empirical methods will be used. Doctrinal analysis will be applied to legal concepts such as 'access to justice', 'privacy' and 'regulation' to clarify how the terms are understood in the evolving technological world of Web 2.0 applications. The research involves analysing what is meant by such terms and at the same time presenting data about how interactive technologies are being used. This will lead to an assessment of whether such applications should be used in the future considering the increased vulnerability of personal data and privacy and the role a secure, regulated environment will play.

Two specific examples of disruptive applications will be explored. The first, the use of OSNs[232] by the Supreme Court of Victoria,[233] particularly the use of Twitter which will be analysed as an example of the way in which courts can use a more open application and the way it is regulated by the Court.[234] The second is the use of eCourtroom[235] as a virtual courtroom, a highly regulated application, in the Federal Circuit Court of Australia and Federal Court of Australia[236]. This is specific technology developed by the Federal Court of Australia in a controlled environment, has been applied primarily to pre-hearing applications.

The empirical methods will involve mixed methodology.[237] This is 'a method and philosophy that attempts to fit together the insights provided by qualitative and quantitative research into

[230] Brownsword, above n 103, 1366.
[231] Ibid 1324.
[232] The Supreme Court of Victoria provides access to its Twitter, Facebook and YouTube posts on its website. As discussed in chapter 7, OSNs can be described as horizontal applications, designed for general use, although in this case used by the Court in a more highly regulated environment.
[233] Supreme Court of Victoria website <http://www.supremecourt.vic.gov.au>.
[234] See Chapter Six of this thesis, 'Strategies for engaging with Web 2.0 applications: resolving the tension'.
[235] Detailed protocols and guides for the use of eCourtroom in the Federal Court and Federal Circuit Court of Australia can be found at <http://www.fedcourt.gov.au >.
[236] See Chapter Five of this thesis, 'Virtual courts facilitating access to justice: an empirical study of eCourtroom'.
[237] Peter Cane and Herbert M Kritzer (eds) *The Oxford Handbook of Empirical Legal Research* (Oxford University Press, 2010).

a workable solution'.[238] The empirical findings and practical consequences of using technology will be used to assist in understanding what future steps should be taken in their application to legal issues. This mixed method process allows a more detailed analysis of the application of innovative technologies in a legal context. Adopting a variety of methods will provide methodological triangulation and complementary information and a stronger evidence base for the research.[239] It has been found by other researchers[240] into information technology and the courts that a variety of methodologies were necessary due to the complex nature of the topic.

While the normative questions being analysed can be placed within a doctrinal context, answers to how interactive technologies are assisting access to justice and what role they may play in the future will be found in the collection of qualitative data within the social context of their application. 'Research designed to secure a deeper understanding of law as a social phenomenon … ' or what has been referred to as 'fundamental research' in law[241] has been acknowledged as an element of broader research categories and methodologies which examine legal processes and other interdisciplinary research.[242] Qualitative methods will be used to provide a more comprehensive analysis of the Web 2.0 applications. The object of the qualitative research will be to examine the Web 2.0 applications in a more detailed way than is possible using quantitative research alone.[243] It is research that can be contrasted with quantitative research and its dependence on statistical quantification.[244] However, the research remains dependent on deductive reasoning.[245]

Webley identified five basic aspects of qualitative empirical research. The first, determining the methodology most appropriate to the research question, such as a survey, questionnaire or interview; second, the selection process; third, how the data is to be analysed, for example by

[238] R B Johnson, and A J Onwuegbuzie, 'Mixed Methods Research: A Research Paradigm Whose Time Has Come; (2004) 33(No7) *Educational Researcher* 14-26.
[239] Terry D Hutchinson, *Researching and Writing in Law* (Thomson Reuters (Professional) Australia Limited, 2010).
[240] Dory Reiling, *Technology for Justice – How Information Technology can support Judicial Reform* (Leiden University Press, 2009) 20.
[241] Social Sciences and Humanities Research Council of Canada, *Law and Learning* (1983) 66.
[242] Australian Council of Deans of Education, *Research Quality Framework: Response to the Issues Paper* (May 2005).
[243] Hutchinson, above n 239.
[244] Lisa Webley, 'Qualitative Approaches to Empirical Legal Research', Chapter 38 in Peter Cane and Herbert M Kritzer (eds) *The Oxford Handbook of Empirical Legal Research* (Oxford University Press, 2010), 926-250.
[245] Ibid.

content analysis, discourse analysis or linguistic analysis; fourth, the ethical considerations; and fifth, the whether the researcher is working alone or with a team.[246]

The use of OSNs by courts such as the Supreme Court of Victoria over a period of three months has been reviewed and analysed using qualitative and quantitative methodology. Two different methods have been applied to the study of eCourtroom which is an application that has been used by the Federal Court of Australia and the Federal Circuit Court of Australia since 2005. The first was based on observation of matters listed during a two month period and a detailed analysis of the type of cases listed and how the matters have been heard by the Deputy District Registrars of the courts. This virtual courtroom was designed as a tool to assist the administrative and legal processes in the court. The system and its development have been described to provide insights and awareness about how such technologies have being applied and to give some indication of their future use. The qualitative data has been supplemented by quantitative data to assist in providing information about how this application enhances access to justice, a description of any issues relating to the disclosure of personal data and what future use may be made of such virtual courts in the future.

A questionnaire was used to elicit personal responses to the use of eCourtroom which was analysed using mainly qualitative content analysis. This method is more commonly associated with research in social sciences than law.[247] Cane and Kritzer acknowledge 'the diversity of empirical investigation of law, legal systems and other legal phenomena'.[248] Qualitative content analysis of judicial opinions and the methodology has been the focus of research in the US,[249] Germany[250] and Australia and has been used to study a broad range of legal subjects.[251] The epistemological roots of content analysis has been linked to Legal Realism and the application of social science tools to analyse the work of the courts.[252] Hall and Wright

[246] Ibid.
[247] Ibid.
[248] Cane and Kritzer (eds), above n 237.
[249] Mark A Hall and Ronald F Wright, 'Systematic Content Analysis of Judicial Opinions' (2008) 96 *California Law Review* 63; Chad M Oldfather, Joseph P Brockhorst and Brian P Dimmer, 'Triangulating Judicial Responsiveness: Automated Content Analysis, Judicial Opinions, and the Methodology of Legal Scholarship' (2012) 64 *Florida Law Review* 1189; Richard A Posner, 'A Theory of Negligence' (1972) 1 *Judicial Legal Studies* 29 which dealt with the coding of trial court records.
[250] Judith Engelke, 'Qualitative Content Analysis of Federal Constitutional Court's Decisions' (Paper presented at Workshop for young researchers, Advocates or Notaries of Democracy? A Comparative Socio-legal Analysis of the Role of Constitutional Courts in Political Transformation Processes, Humboldt University, Berlin, 22 September 2011) <https://www.bgss.hu-berlin.de/de/bgss/bgssonlinepublications/.../paper3neu>.
[251] Hall and Wright, above n 249, 73.
[252] Ibid 76.

do not consider that content analysis is tied to 'any particular jurisprudential school, other than to positivism in the broadest sense'.[253] The strength of the methodology has been identified as providing objective understanding.[254] The distinct components of content analysis outlined by Hall and Wright include the selection process, coding and analysis. The selection process, in contrast to interpretive legal scholarship, specifies 'replicability'.[255]

Webly considered that classical content analysis has wide application and can be applied to 'legal phenomena within press reports or legal cases, or to consider the content of interview or policy documents'.[256] She discussed the use of computer-assisted analysis, using programs such as NVivo[257] and Atlas[258], which could help to make the coding process more systematic but commented that the researcher still played an important role in the selection of codes and the interpretation of relationships between them.[259] It has not been considered appropriate to analyse OSNs by using software such as Klout[260] and Gephi[261] for this dissertation.[262] Such online programs provide the capacity to assess the extent of interaction between participants in a graphic and quantitative manner. The use of these programs is more appropriate for quantitative research, particularly when large numbers are involved. The Twitter site itself indicates the number of people following the twitter posts and other similar indicators which provides some indication of interaction without using analytical ranking. A smaller sample has been chosen in the current analysis and examined from a qualitative perspective. The specific use of Twitter by the Supreme Court of Victoria will be discussed in the context of the general disruptive nature of OSNs in Chapter Four.

[253] Ibid 77: they qualify this to mean *"logical* positivism, the basic philosophical view of the world underlying modern science, as opposed to *legal* positivism, which examines factors that determine the legitimacy of law".
[254] Hall and Wright, above n 238, 141. Hall and Wright have applied their methodology to the analysis of judicial opinions and have developed "a common law of case coding" implementing best practices and applications, 121.
[255] Ibid 79.
[256] Webley, above n 244, 17.
[257] Ibid.
[258] Ibid.
[259] Ibid.
[260] The Klout Score created uses a number from 1 to 100 to rank "social influence". Klout uses social media analytics to rank user's interactions in online social networks < http://www.klout.com>.
[261] This is an open graph visualization and exploration platform used to assist data analysis and discover patterns, a complementary tool to traditional statistics <http://www.gephi.org>.
[262] I considered adopting computer-assisted analysis when I attended the 5th International Conference on Communities and Technologies at the Queensland University of Technology, Brisbane on 29 June 2011. The Workshop, 'Making Sense of Twitter: Quantitative Analysis Using Twapperkeeper', chaired by Axel Bruns and Jean Burgess described the strengths and limitations of using computer analysis. I concluded that computer analysis would be more suitable to large scale quantitative analysis.

Finding adequate assessment tools for access to justice and privacy have proven elusive and in part due to the difficulties of identifying the elements to be measured. There have, however, been extensive attempts to measure access to justice over recent years. Some scholars have questioned whether it is possible to make access to justice a 'quantifiable concept rather than a broad aspiration'.[263] While designing precise measurement tools for concepts such as 'justice', 'privacy' and 'openness' has proven challenging, however, there has been an acceptance that whatever tools are chosen, whether composite indices, program logic models, qualitative or 'quantitative measures from perceptual surveys', they will all have their limitations.[264]

The 'absence of common terminology about access to justice, mechanisms to measure change, and a practical definition of success' were seen as barriers impeding improvements to access to justice.[265] It has been considered necessary to reach a common understanding of 'the components of access to justice' so that performance measurements or 'access to justice metrics' could be developed.[266] The discussion paper referred to eleven access to justice objectives identified in the literature.[267] Although it was considered difficult, it was stated that access to justice metrics required measurement and reporting on inputs, outcomes and the 'relationship between the two'.[268] The various initiatives in the past ten years to find an evidence base for global indicators of the justice system and thereby provide international comparisons and evidence about effectiveness of reforms include: the Worldwide Governance Indicators[269]; the Rule of Law Index;[270] Measuring Access to Justice;[271] International

[263] Martin Gramatikov, Maurits Barendrecht and Jin Ho Verdonschot, 'Measuring the Costs and Quality of Paths to Justice: Contours of a Methodology' 3 (2011) *Hague Journal on the Rule of Law* 349-379, 350.
[264] Elizabeth Shearer, 'An evidence base for the federal civil justice system' (2011) *Managing Justice* 21 <http://www.managingjustice.com.au>.
[265] Canadian Bar Association, 'Access to Justice Metrics: Discussion Paper' (2013) <http://www.cba.org> 1.
[266] Ibid.
[267] Ibid 4: these objectives detailed are references to the work of John Lands, 'A Guide for Policymaking that Emphasizes Principles, and Public Needs' in 26:11 (2008) *Alternatives to the High Cost of Litigation* 197:, 1. Promoting substantive and procedural fairness; 2. Satisfying disputant's substantive interests; 3. Satisfying disputants with the dispute resolution process itself; 4. Reducing risks related to disputes; 5. Reducing harm to disputants and others, including society generally; 6. Providing greater choice in dispute resolution processes for disputants and ADR professionals; 7. Increasing disputants' capabilities to handle other disputes; 8. Promoting productive relationships between disputants; 9. Satisfying disputants with the services of dispute resolution professionals; 10. Improving the culture of disputing for disputants, professionals, and society, and 11. Promoting compliance with social policies expressed in the law, such as non-discrimination.
[268] Ibid 6.
[269] This was an initiative by the World Bank which reported on 213 economies using perception based data from individuals and provided index scores <http://info.worldbank.org/governance/wg/index.asp>.
[270] This was a World Justice Project which reported on 35 countries and included data on access to the civil justice system. It provided index scores and used survey data from users. <http://worldjusticeproject.rog/rule-of-law-index>.
[271] This was research by the Hague Institute for the Internationalisation of Law, Tilburg Institute for Interdisciplinary Studies of Civil Law and Conflict Resolution which used a survey tool to collect information

Framework for Court Excellence;[272] the Australian Report on Government Services – Court administration[273] and the Legal Needs Surveys.[274] This research has been described and assessed by Shearer.[275]

In the UK, the Legal Services Board considered a range of indicators to evaluate access to justice as a guide to measuring the impact of reforms introduced against the regulatory objectives set and so improve access to justice.[276] The focus of this research was individual consumers. The 2006-09 Civil & Social Justice Survey[277] was used to analyse civil and social justice problems over three years. It was found that a 'basket of indicators' would be needed to assess such a complex concept as access to justice with a consideration of an 'array of different individual elements'. However, because data was found to be scarce, particularly relating to the legal services market, it was considered important to use existing published data and existing research. It was also thought that it would be useful to determine trends in the number of websites providing legal advice to assess the impact of technology, however, it was not considered a practical measurement to obtain because there has not been mandatory registration process for such websites. Similarly data on the number of non-parties attending court proceedings, either in person, viewing or reading court materials online is not available as an indicator of the openness of court proceedings.

The emphasis on cost savings and efficiencies have led to a search for the perfect but illusive index. As found in the World Justice Project, there are strengths and limitations in all attempts. The strengths in the World Justice Project Rule of Law Index was found to be in its comprehensiveness, its basis on new data, its focus on law in practice and actual experience, however it was concluded that:

from users of the formal and informal justice systems. It collected data on access to justice <http://measuringaccesstojustice.com>.

[272] This was research by the United States Federal Judicial Centre & National Centre for State Courts, the Subordinate Courts of Singapore and the Australian Institute of Judicial Administration – this research used self-assessment questionnaires and gathered data on the quality of justice covering formal and informal justice systems <http://www.measuringaccesstojustice.com>.

[273] This was research by the Productivity Commission and measured State and Commonwealth Courts performance in Australia, their equity, effectiveness, including quality and access, and efficiency using a common set of output measurements.

[274] This research was conducted by various agencies in the UK, USA, Canada, New Zealand and the Law and Justice Foundation. It consisted of surveys to describe the incidence of legal problems covering the formal and informal justice system.

[275] Shearer, above n 264.

[276] 'Evaluation: How can we measure access to justice for individual consumers?' A discussion paper (September 2012) Legal Services Board <http://www.legalservicesboard.gov.uk>.

[277] Civil Justice in England and Wales: Report of the 2007 English and Welsh Civil and Social Justice Survey, LSRC, 2008.

> The Index is a diagnostic tool that provides a general assessment of the health of the rule of law in a given country at a particular moment in time. It does not explain the causes of the conditions it describes, nor does it prescribe remedies. In addition, no single index can convey a full picture of a country's situation. Rule of law analysis requires a careful consideration of multiple dimensions that every from country to country and a combination of sources, instruments, and methods. [278]

The Index is limited in that it can provide a general assessment only without prescribing solutions. The complexity of the problem has been also reflected in other approaches adopted to determine a methodology for assessing justice. These have included ones which measure specific jurisdictions, specific pathways, indexes, and various consolidated approaches. They have revealed the challenge of transforming a concept into a quantifiable entity particularly when there is little agreement about what the term 'access to justice' means. One approach has concerned measuring aspects of the rule of law or estimating 'inputs'. Few have measured the perceptions of the end users due to the difficulty of assessing emotional cost, perceptions of the quality of the procedures, outcome or finding a systematic way of measuring people's experiences of the justice system[279].

The conceptual and methodological challenges in measuring costs and quality of access to justice have been summarised by Gramatkov et al, drawing on the research of Braendrecht, Mulder et al in 2010 and The Hague Model[280] of measuring access to justice. This model identified twelve categories of legal problems that appeared urgent in most legal systems and set out parameters for measuring 'cost and quality of access to justice'. Researchers aimed to create an internationally valid benchmark. Barendrecht et al[281] discussed the legal problems and needs of individuals in a broad sense in their twelve categories.[282] It was recognised that

[278] Mark D Agrast et al, *The World Justice Project: Rule of Law Index 2012-2013* (2012) World Justice Project <http://worldjusticeproject.org/publication/rule-law-index-reports/rule-law-index-2012-2013-report>.
[279] Gramatikov, Barendrecht and Verdonschot; above n 252, 350.
[280] Hague Institute for the Internationalisation of Law (HiiL), *Measuring Access to Justice in a Globalising World: The Hague Model of Access to Justice Rule of Law*– Final report (April 2010). Measuring access to justice is one of the first five research projects supported by the HiiL. The development of a methodology for measuring access to justice from the perspective of the users was developed by the Tilburg Institute for Interdisciplinary Studies of Civil Law and Conflict Resolution Systems <http://www.hiil.org/publication/measuring-access-to-justice-in-a-globalising-world%20-%20report>.
[281] Baurits Barendrecth, Peter Kamminga and Jin Ho Verdonschot, 'Priorities for the Justice System: Responding to the Most Urgent Legal Problems of Individuals', TISCO Working Paper Series on Civil Law and Conflict Resolution Systems', No 001/2008 (February 5, 2008, Version: 1.0) <http://ssrn.com>.
[282] Ibid. The 12 categories used were: 1. Subsistence problems; 2. Basic personal security; 3. Property rights protection; 4. Identity issues and documents; 5 Problems in land use relationships; 6 Problems in employment relationships; 7 Problems in family relationships; 8 Problems in neighbour relationships; 9 Problems with sellers of goods and services; 10 Business problems; 11 Debt problems; 12 Problems with financial services

surveys of legal needs may not realistically reflect legal problems because individuals may not realise that a problem is a legal issue and they also do not indicate problems that are dealt with by a well-functioning legal system.[283] They concluded that 'legal needs surveys show a broad variety of legal problem, with a focus around certain key relationships'.[284] Some indication of the most important legal problems for average individuals emerged from this study. Those relating to basic personal security and issues relating to family and employment are considered among the most important. Complaints such as those about the quality of goods and debt problems are frequent but are not regarded as sufficiently disruptive or urgent.[285]

The primary units of analysis adopted for the research design of Gramatkov's team were related to paths to justice.[286] The users of justice are asked to assess the procedure and its outcome not the functioning of the legal system. The first instance judicial proceeding were seen as one path and an appeal as a separate path, although it was thought possible to include the appeal and measure the whole process.

In presenting a methodology for measuring costs Gramatikov aggregated individual costs into tangible (monetary costs) and intangible costs.[287] Attempts to measure costs of solving disputes have been common probably because the cost of litigation has been the most frequently discussed of the barriers of access to justice and it was viewed by Lord Woolf as the 'most serious problem' of the litigation system.[288] The methodology for measuring the impact of technology is limited to specific developments and has not included OSNs and their interaction with law, other than as a general consolidated index representing access to justice. There has been limited specific research on the digital pathway to justice.

[283] Ibid 11-12.
[284] Ibid 37.
[285] Ibid.
[286] Martin Gramatikov, Maurits Barendrecht and Jim Ho Verdonschot, 'Measuring the Costs and Quality of Paths to Justice: Contours of a Methodology' (2011) 3 *Hague Journal on the Rule of Law* 349, 358: the term "path to justice" was defined as *a commonly applied process which users address in order to cope with their legal problem.* This is a broad definition encompassing formal and informal paths, including adjudication, arbitration and negotiation. It begins when a person takes the first steps to resolve a legal problem, including searching for information. The end of the path is "*the moment of a final decision by a neutral, joint agreement of the parties, or an end to the process because one of the parties quits the process."*
[287] Martin Gramatikov, 'A Framework for Measuring the Costs of Paths to Justice' (2009)2 *The Journal Jurisprudence* 111-147, see also <http://ssrn.com/abstract=1279397>.
[288] Lord Woolf, *Access to Justice Final Report to the Lord Chancellor on the Civil Justice System in England and Wales* (H M Stationery Office, 1996).

While there are general limitations to the application of quantitative assessment to a concept such as 'access to justice' and the development of a specific index, it is possible that recommendations concerning qualitative assessment and a list of characteristics for evaluation may provide a valuable framework for the assessment of the effectiveness of using innovative applications. This idea will be explored in more detail in the final chapter of this thesis.

1.6 – Structure of the thesis

In this chapter I have discussed the innovative developments of Web 2.0 and the regulatory context for my research. It is a complex regulatory environment challenging fundamental legal concepts and principles. The use of Web 2.0 has provided a communication platform for access to courts and the promise of a digital pathway to justice. The technological developments have enabled tools for searching; tools to filter the internet's 'avalanche of data'; and tools for collaboration which empower 'people and organisations to transform data by 'mashing it up', combining it with other data' to make it useful in different ways.[289] The use of the new collaborative tools of Web 2.0 has been recognised as offering 'an unprecedented opportunity to achieve more open, accountable, responsible and efficient government'.[290]

The opportunities offered for the courts include more open access, efficiencies and cost savings, however, Web 2.0 has introduced a new regulatory environment where privacy and access are in apparent conflict as the demands for and the availability of personal information is driven by commercialisation of the internet making such data a valuable commodity. The retention of personal data has become an incentive for economic gain. 'Privacy' and 'access to justice' have become concepts in conflict in an era of rapid technological change and globalisation.

There has been limited research on the impact of innovative applications on courts and the legal system, much of it focussing on the negative impact and dangers that OSNs have presented for lawyers, judges and the courts rather than on the benefits, particularly in the direct communication that it provides. An evidence-based analysis, common in fields such as medicine and criminal law has been described as being 'notably absent from the many efforts

[289] Nicholas Gruen, 'Engage: Getting on With Government 2.0' Vol 2 Chapter 28 in Brian Fitzgerald (ed) *Access to Public Sector Information: Law, Technology & Policy* (Sydney University Press, 2010) 615-629, 615.
[290] Ibid 616.

to expand access to the justice system' and from an analysis of civil legal problems to explain the sort of interventions that work for litigants.[291]

The methodology chosen to analyse the digital pathway promised by the innovative applications of Web 2.0 is a combination of theoretical analysis and empirical research. The theoretical analysis provides a context for the analysis of 'access to justice' and the issues accompanying the disclosure of personal data online. The empirical research assists in evaluating the use of disruptive innovations by the courts to provide increased access and the methods adopted to protect personal data.

Chapter Two contains the theoretical analysis on access to justice and a discussion of the relevant literature and research, particularly digital access and the access to justice movement. The evolving conceptual changes in what 'access' means in the digital era has implications for the legitimacy of technological regulation. These changes also have impacted on the nature of open courts, due in part to the paradigm shift in digital communication.

In Chapter Three I have examined the changing nature of online legal information in the digital world and the tension between the openness made possible by Web 2.0 applications and the protection of personal data. While the principle of open courts retains its fundamental role in the administration of justice, the increased availability of information and personal disclosure together with the cross-border flow of data has increased the pressure on policy makers to adapt to the changes. Court records have become 'aggregated repositories of information about people'[292] as they are moved online. While the right to privacy has received some acceptance and acknowledgment in international documents, finding a common understanding has proven elusive with definitions confined to 'personal information' and 'personal data'. Considerable regulatory challenges have arisen in the new technological environment for the control of personal data.

The disruptive nature of innovation that facilitates disclosure of personal data and interference by third parties with is presented in Chapter Four through an analysis of OSNs and their interaction with the legal systems. This analysis included the issues of confidentiality and ethical problems faced by the legal profession in using OSNs. The analysis of the use of

[291] Laura K Abel, 'Evidence-Based Access to Justice' (2009) 13 *University of Pennsylvania Journal of Law and Social Change* 295-313, 295.
[292] Amanda Conley et al, 'Sustaining both Privacy and Open Justice in the Transition from Local to Online Access to Court Records: A multidisciplinary Inquiry' (2012) 71 *Maryland Law Review* 772-847, 846.

Twitter, by the Supreme Court of Victoria enabled a contrast to be drawn between specifically designed applications in a controlled context with applications more generally available. The analysis focussed on the limitations of interaction in the context of the administration of justice.

A detailed empirical analysis of a disruptive, interactive application, eCourtroom, used by the Federal Court of Australia and the Federal Circuit Court of Australia has been presented in Chapter Five. Virtual courtrooms which provide the future digital pathway has been used to demonstrate the exigent issues for courts and the legal system in Australia and the implications of their use for privacy, security and access to justice. The regulatory environment within the courts has been contrasted to more complex environment of online social networks discussed in Chapter Four. The need for continual evaluation and modification to the use of such applications has been explored.

The research question has been revisited in the closing chapter and constructive strategies for engagement with the regulatory demands of Web 2.0 applications explored. A review of possible regulations and the legal regulatory framework to provide the necessary privacy for the future has been proposed as well as suggestions for future research. The implications for legislative legitimacy and effectiveness have necessitated a search for boundary markers to define the limits of open access. With increased openness and transparency personal data is more exposed in the altered regulatory environment of digital era and this has necessitated re-examination of the strategies for engaging with Web 2.0 applications. Legislative changes, the development of a digital access to justice index and the adoption of the EU concept of privacy as based on human dignity have been considered as possible options for the future.

A multidisciplinary approach has been adopted to provide a new perspective on the use of technology in law, although the adoption of such an approach can present both practical and philosophical challenges. Some of the practical problems include limited training in the methodologies of other disciplines, an absence of data, as well as logistical challenges such as the appropriate journal for publication of results. More fundamental problems have been identified by Owen and Noblet including a view that such multidisciplinary research can threaten traditional values and skills.[293] Conley et al presented an analysis of privacy and open justice integrating legal, philosophical and technical disciplines, although they admitted that

[293] Dave Owen and Caroline Noblet, 'Interdisciplinary Research and Environmental Law' (2014) 41 *Ecology Law Quarterly* 887-938.

the limitation may be that the paper did not 'embody the traditional form of any one of them'.[294] Also Tan and Hsiao found in assessing the disadvantages of multidisciplinary collaboration that time constraints due to the need to communicate and respond was a limitation, as well as they identified that there were disadvantages caused by the different background of collaborators and therefore a different understanding of the work.[295]

The following chapter, Chapter Two, presents an analysis of the nature of justice online in the digital context in which Web 2.0 applications are to be found and the way in which access to justice has been transformed by open access and transparency inherent in Web 2.0.

[294] Conley et al, above n 292, 777.
[295] Hsien-Hui Tang and Emily Hsiao, 'The advantages and disadvantages of multidisciplinary collaboration in design education' (Paper presented at the International Association of Societies of Design Research, Tokyo, 2013) <http://www.design-cu.jp/iasdr2013/papers/1459-1b.pdf>.

Chapter Two: Access in the digital era

2.1 Introduction

In addressing the question of the extent to which Web 2.0 applications can be used to enhance access to justice, a theoretical analysis of what access to justice means in the digital era is fundamental. The digital era is characterised by openness and transparency which may increase 'access' but not necessarily 'access to justice'.

The phrase access to justice itself appears to infer that access and justice are complementary, so that the more access that is provided the greater the justice. There is also an implication that with access there is also an accompanying openness and transparency. Access and open justice are concept in apparent harmony, despite some degree of linguistic indeterminacy in the terms themselves. However, the apposition of access and justice, as well as open and justice can be mesmerising, as Ormrod LJ found in *Norwest Holst Ltd v Department of Trade*[296] in relation to the apposition of natural and justice.

A useful starting point in an analysis of access to justice is that of Lord Neuberger in his discussion of the relationship between justice and the rule of law. He adopted a narrower meaning of the rule of law, that is, it is 'effective access to the courts for citizens to protect and enforce their fundamental rights' with a focus on 'accessibility to the law and accessibility to the courts'.[297] He rejected the idea attributed to modern civil justice reform, that there can be access to justice when there is a 'diversion of disputants away from the courts'.[298] For Lord Neuberger, access to justice consisted of eight elements:

> First, a competent and impartial judiciary; secondly, accessible courts; thirdly, properly administered courts; fourthly, a competent and honest legal profession; fifthly, an effective procedure for getting a case before the court; sixthly, an effective legal process; seventhly effective execution; eighthly, affordable justice. [299]

[296] *Norwest Holst Ltd v Department of Trade* [1978] Ch 201, 226. In this case the phrase 'the requirements of natural justice' was considered in the context of the discretionary power of the Minister to appoint inspectors of the Department of Trade. Lord Justice Ormrod considered that the word 'natural' added nothing except nostalgia and '[i]n many cases … the two are synonymous but not by any means in all'. In addition, in referring to findings of the House of Lords and the Court of Appeal, it had been found that 'the principles of natural justice must be kept flexible and must be adapted to the circumstances prevailing in any particular case'.

[297] Lord Neuberger, P, 'Justice in an Age of Austerity' (Paper presented for the Tom Sargant memorial lecture 2013, London, 15 October 2013) https://www.supremecourt.uk/docs/speech-131015.pdf 3.

[298] Ibid. Lord Neuberger refers to the comments by Dame Hazel Genn, *Judging Civil Justice* (*The Hamlyn Lectures 2008)* (Cambridge University Press, 2010) where she was reported as saying it was 'hard not to draw the conclusion that the main thrust of modern civil justice reform is about neither access nor justice. It is simply about diversion of disputants away from the courts. It is essentially about less law and the downgrading of civil justice' 9.

[299] Ibid 11.

He considered, in essence, that the essential requirements of the rule of law consisted of access to the courts to have claims heard and to have a determination by judges in public according to the law.[300]

Access to justice has been described by Lord Bingham in a similar manner as in the analysis of Lord Neuberger. It was seen as having considerable significance for the rule of law.[301] The essential components being that 'the law must be accessible and so far as possible intelligible, clear and predictable',[302] there must be an opportunity provided for resolving disputes so that 'everyone is bound by and entitled to the benefit of law … [and] … be able, in the last resort, to go to court and have their rights and liabilities determined'; and there must be recognition of 'the right of unimpeded access to a court as a basic right, protected by domestic law'.[303]

Smith, in the context of the provision of legal aid, considered that access to justice needed to be more than an 'anodyne version' or 'totally debased' phrase. [304] Detached from its origins, some authors have found it to be completely meaningless.[305] I will examine the use of the phrase access to justice and why, rather than ignoring it, identification of its roots and context can facilitate a detailed analysis of the courts' transition to the digital environment. The boundaries of my analysis will be digital access to justice which can be contrasted to the more general and broader use of the phrase to refer to legal justice and social justice often used within the confines of political and policy discourse. It is not possible to discuss each aspect of access to justice in detail. Most of the components are interdependent. In order to find a workable definition for access to justice for the analysis of the use of innovative technologies in this thesis, the concept will be located within the context of the digital era. My focus will be on those aspects of most relevance to technological innovation to determine the boundaries, if any, that need to be placed on its use. It is the accessibility of courts, the effective procedures

[300] Ibid.

[301] Lord Bingham, 'The Rule of Law' (2007) 66 *Cambridge Law Journal* 67-85.

[302] Ibid 67.

[303] Ibid.

[304] Roger Smith, 'After the Act: what future for legal aid?' (2012) 9(2) *Justice Journal* 8-23, 17. This article was delivered as the Tom Sargant memorial annual lecture 2012, London, 16 October 2012. Roger Smith is an honorary professor of Kent University and a visiting professor at London South Bank University and has worked for various non-government organisations, including the Legal Action Group, the Child Poverty Action Group and the Law Society. He is a former director of Justice. Justice was founded in 1957 by leading jurists to promote the rule of law and fair administration of justice and is an all-party law reform and human rights organization comprising barristers, solicitors, legal executives, academic lawyers, law students and interested non-lawyers <http://justice.org.uk>.

[305] Jon Robins, 'Access to justice is a fine concept. What does it mean in view of cuts to legal aid?' *the guardian* (online), 6 October 2011 <http://www.theguardian.com/law/2011/oct/06/access-to-justice-legal-aid-cuts>.

and processes that can be provided by Web 2.0 application that is in issue. Therefore access to justice can be defined for present purposes as: digital access to courts with open, effective procedures and processes for the determination of claims and access to information about the law.

2.2 Whose access to which justice?

The phrase access to justice appears to suggest that once there is access there is also justice. However, as Sage-Jacobson has discussed, that in any analysis of the concept access to justice the conceptual concern remains, 'whose access to which justice'.[306] She considered that there has been a lack of understanding of the legal needs and the aims of the civil justice system. Sage-Jacobson advocated not only addressing the underlying conceptual concerns but also called for comprehensive evidence of the public expectations of civil justice rather than a '"demand and supply" economic modelling'.[307]

It has been argued that 'there are two paths of access: one to legal justice and another to social justice, which are overlapping but not synonymous.'[308] While the concept may have many different meanings, it has been stated that the basic assumptions are similar. The goal is 'justice' and it is the door to 'justice' that is closed for some individuals or groups in society.[309] These groups may include the poor or disadvantaged, a racial minority, or certain ethnic groups or, as found by more recent research, may include the middle income group.

Access to justice is a concept that is easily spoken about but more difficult to realise or even achieve 'consensus on its meaning'.[310] The meaning of the phrase access to justice was once considered too obvious for a definition with an assumption that it was synonymous with access to courts, until the 1970s with the development of the access to justice movement. This began with a most comprehensive comparative analysis of the challenges to modern legal

[306] Susannah Sage-Jacobson, 'The Ongoing Search for a Demand-Side Analysis of Civil Justice in Australia', Chapter 5 in *Australian Courts: Servicing Democracy and its Publics*, The Australasian Institute of Judicial Administration Incorporated, Melbourne, 2013) 49-67, 64.
[307] Ibid 49.
[308] Mauro Cappelletti and Bryant G Garth (eds) Volume I, *Access to Justice. A World Survey* (Sijthoff and Giuffrè, 1978).
[309] Mauro Cappelletti and John Weisner (eds) *Access to Justice: Promising Institutions* Vol 2 Part 1 (Sijthoff and Noordhoff, 1978), 5.
[310] Patricia Hughes and Janet E Mosher (eds) 'Forward' (2008) 46 *Osgoode Hall Law Journal* xxix-xxxv, xxix.

systems, the Florence Access-to-Justice Project.[311] Access to justice was analysed by reference to purpose and within the context of the reform agenda:

> The words access to justice are admittedly not easily defined but they serve to focus on two basic purposes of the legal system – the system by which people may vindicate their rights and/or resolve their disputes under the general auspices of the state. First, the system must be equally accessible to all, and second, it must lead to results that are individually and socially just. Our focus here will be primarily on the first component, access, but we will necessarily bear in mind the second. Indeed, a basic premise will be that social justice, as sought by our modern societies presupposes effective access.[312]

The two basic purposes of the legal system identified were that it should be accessible by everyone and lead to results which are just for the individual and society generally. The Florence Access-to-Justice Project has had considerable influence on most subsequent analyses and proposals for legal reform. Cappelletti and Garth have explained how these rights were transformed in the welfare state in the second half of the twentieth century into substantive rights from the theoretical conception of access to justice in the late eighteenth and nineteenth centuries.[313] It was considered to be a natural right of access to the courts. It was not a right protected by the state and only available to those who could afford to use it.

Cappelletti and Garth linked effectiveness and access:

> Effective access to justice can thus be seen as the most basic requirement – the most basic "human right" – of modern, egalitarian legal systems which purports to guarantee, and not merely proclaim the legal rights of all.[314]

What Cappelletti considered was not so clear was an understanding of the concept of 'effectiveness'. The perfect equality or 'optimal effectiveness' was seen as 'utopian' and could not be achieved because it would never be possible for the outcome of a dispute to depend only on the relative merits of the opposing positions rather than the strengths of the opposing parties.[315]

In reform proposals for the civil justice system over the past thirty years, the term access to justice has possibly been one of the most discussed terms. It has been viewed as of

[311] This project was funded by the Ford Foundation and the Italian National Research Council. Reports were produced between 1973 and 1978 on the quality of justice, access to justice and legal aid and a report on the "access-to-justice movement in four volumes.

[312] Cappelletti and Garth, above n 308, 6.

[313] Ibid 6-7.

[314] Ibid.

[315] Mauro Cappelletti, Bryant Garth and Nicolò Trocker, 'Access to Justice: Comparative General Report (1976) 40 *The Rabel Journal of Comparative and International Private Law* 669, 680.

fundamental importance to a modern legal system, although difficult to define other than by what it can achieve. Having begun as a concept narrowly confined to the formal legal system, it has developed a much broader meaning encompassing more informal dispute mechanisms as well as justice in daily life. It can be limited to process, or interpreted as 'encompassing substantive elements'.[316] It is a concept that can be defined from the perspective of the users of the system, those who are participating in the legal system (the parties and legal profession) and from the perspective of those who need to evaluate it (the public). Sandefur considered access to justice as 'an object both of scholarly inquiry and political contest, and both a social movement and a value commitment that motivates study and action'.[317]

As mechanisms of redress became more diversified the definition has become broader and included more than access to the courts.[318] Bedner and Vel proposed a process definition for access to justice:

> Access to justice exists if:
> - People, notably poor and disadvantaged,
> - Suffering from injustices
> - Have the ability to make their grievances be listened to
> - And to obtain proper treatment of their grievances
> - By state or non-state institutions
> - Leading to redress of those injustices
> - On the basis of rules or principles of state law, religious law or customary law
> - In accordance with the rule of law.[319]

This definition stressed the capacity for people to have their problems heard and remedied. Later definitions which refer to institutions other than the courts and to informal processes usually acknowledge the influence of the court system and the use of alternate dispute resolutions as being undertaken in the 'shadow of the law'.[320]

To understand what access to justice means most often follows a contextual inquiry, whether this is within the context of gender, race, skills, nationality, time periods, financial constraints

[316] Hughes and Mosher, above n 310.

[317] Rebecca L Sandefur (ed) *Access to Justice: Sociology of Crime, Law, and Deviance* vol 12, 'Access to Justice: Classical Approaches and New Directions' (Emerald/JAI Press 2009) ix.

[318] Adriaan Bedner and Jacqueline A C Vel, 'An Analytical framework for empirical research on Access to Justice' 2010 (1) *Law, Social Justice & Global Development Journal*, 1-29, 4.

[319] Ibid 7. This definition of access to justice was originally developed by Jan Michiel Otto and modified by Bedner and Vel.

[320] This expression refers to the 'impact of the legal system on negotiations and bargaining that occur *outside* the courtroom': See Robert H Mnookin and Lewis Kornhauser, 'Bargaining in the Shadow of the Law: The Case of Divorce' (1979) 88 *The Yale Law Journal* 950-997,950; the term has also been described as 'pretrial bargaining' where a game is played in the shadow of the law with two possible outcomes: 'settlement out of court through bargaining, and trial, which represents a bargaining breakdown'. The courts have been described as encouraging 'bargaining but stand ready to step from the shadows and resolve the dispute by coercion if the parties cannot agree': See Robert Cooter, Stephen Marks with Robert Mnookin, 'Bargaining in the Shadow of the Law: A Testable Model of Strategic Behaviour' (1982) 11 *Journal of Legal Studies* 225-251, 225.

or social status. A study of access to justice in late medieval England, for example, found that literacy was 'a necessary precursor to accessing justice', in particular the ability to read and write in Latin. Clerks and scriveners – the 'technology' of the day – provided the practical and procedural means of access.[321] However, an analysis of numerous access to justice reports since the 1970s, when literacy was no longer such an issue, indicates a focus on those in society who were unable to fund litigation and who were dependent on legal aid provided by government budgets.

It has been a concept used often in association with the reform of justice systems in response to perceived crises, particularly in civil justice systems. Such reforms are on-going as developments in society and new proposals for change emerge. The concept has been adapted to meet the emerging challenges. Justice Sackville has referred to the expression 'access to justice' as 'ubiquitous in legal and political discourse',[322] one that survives because of its diverse meaning.[323] He evaluated six assumptions[324] underlying the access to justice movement in an attempt to create a realistic expectation of what can be achieved. He considered it was important to recognise the limitations of courts and tribunals to balance the 'rhetoric of access to justice' and formulate the 'right policy questions'.[325]

Hughes and Mosher considered access to justice as a concept with 'elasticity' representing a number of ideas often changing with context.[326] One of the contexts explored by Hughes was law reform commissions. Hughes considered that law commissions were more suited to addressing broader issues, making recommendations that 'enhance justice beyond law' and contributing to the dialogue about the meaning of access to justice.[327] Hughes commented 'that it is inherent in the notion of a contemporary law commission in a liberal democracy …

[321] Kitrina Lindsay Bevan, 'Clerks and Scriveners: Legal Literacy and Access to Justice in Late Medieval England' (March 2013) thesis submitted for the degree of Doctor of Philosophy in Law, University of Exeter, <https://ore.exeter.ac.uk/repository/handle/10871/10732> 17.

[322] Ronald Sackville, 'Some Thoughts on Access to Justice' (Paper presented at the First Annual Conference on The Primary Functions of Government Courts, Faculty of Law, Victoria University of Wellington, New Zealand, 28-29 November 2003): (2003) 22 (FCA) *Federal Judicial Scholarship* <http://www.austlii.edu.au>.

[323] Ibid.

[324] Ibid. These assumptions were: first, that 'the courts can be relied on to vindicate the rights and protects the interests of the disadvantaged individuals and groups in a timely and cost-effective manner'; second, that the authority of the courts is beyond challenge; third that governments are able to devote sufficient resources to legal aid services; fourth, that increased access is an unqualified good; fifth, that the best way forward is the replacement of 'dependence by many people on the favourable exercise by public agencies or public officials of unfettered administrative discretion with entitlements'; and sixth, that the provision of services will remain the province of the government.

[325] Ibid.

[326] Hughes and Mosher, above n 310, xxix.

[327] Patricia Hughes, 'Law Commissions and Access to Justice: What Justice Should We Be Talking About? (2008) 46 *Osgood Hall Law Journal* 773-806, 806.

that it be concerned with questions related to enhancing access to justice, broadly defined'.[328] This is illustrated by the listed objectives of the Australian Law Reform Commission (ALRC).[329]

Conklin[330] examined the 'tradition of "access to justice" studies' finding five models of access to justice, each with a structure separating 'valid legal rules/principles from a non-law' or morality.[331] The five models place justice external to the legal structure. This Conklin viewed as the legal reality. In the first model[332] 'justice is associated with a pure procedure' and there is no justice independent of the procedure of reaching a decision, so that if the procedure is fair then all participants gain access to justice and the 'substantive content of the outcome of the procedure need not matter'. In the second model[333] the 'institutional source of the outcome' is important not the procedure and what matters is that the institution has the 'proper jurisdiction to enact the rule'. The third model[334] is a semiotic model where access to justice involves 'an access to a special legal language with a complex vocabulary and grammar', justice being dependent on the interpretation of a phrase or sign such as 'reasonable time' which has a very special significance in legal language. Justice in these three models, Conklin claims, is 'excluded, discarded, an impossibility, forgotten and then inaccessible'. Justice in the fourth model[335] is associated with the unspoken and unwritten social practices of a community. Justice is seen as inaccessible also in this model because access to justice 'exists on faith'. The fifth model[336] is referred to as the 'law and … ' model where justice is outside the legal structure and access to justice obtained by examining law 'through literature or feminism or the "other" disciplines'. This analysis leads to a deeper understanding of justice in a broad context and suggests that an understanding of access to justice in the digital era is not to be found in the access to justice movement but outside this structure.

[328] Ibid, 775.

[329] The Australian Law Reform Commission is a federal agency operating under the *Australian Law Reform Commission Act 1996* (Cth) and the *Public Governance, Performance and Accountability Act 2013* (Cth) which conducts inquiries into areas of law at the request of the Attorney-General of Australia. It monitors overseas legal systems to ensure 'international best practice' and has regard to the effect of its recommendations on the 'costs of access to, and dispensing of, justice'. Providing improved access to justice is one of its listed objectives. The other objectives include: bringing the law into line with current conditions and needs; removing defects in the law; simplifying the law; and adopting new and more effective methods for administering the law and dispensing justice, <http://www.alrc.gov.au/about>

[330] William E Conklin, 'Whither Justice? The Common Problematic of Five Models of "Access to Justice"' (2001) 19 *Windsor Yearbook of Access to Justice* 297.

[331] Ibid.

[332] Ibid 298-300.

[333] Ibid 300-305.

[334] Ibid 305-309.

[335] Ibid 309-311.

[336] Ibid 311-313.

In contrast to definitions of access to justice in developed countries, the concept in the context of developing countries such as Indonesia, has had a different focus, particularly as state courts and institutions have not played a similar role to courts in western countries. The Access to Justice in Indonesia Project[337] has adopted what is referred to as a process definition[338] which focuses on the process the justice seeker must experience to achieve appropriate redress. The definition sets out to include people who are poor and vulnerable and who suffer from injustices in their daily lives.

> Access by people, in particular from poor and disadvantaged groups to fair, effective and accountable mechanisms for the protection of rights, control of abuse of power and resolution of conflicts. This includes the ability of people to seek and obtain a remedy through formal and informal justice systems, and the ability to seek and exercise influence on law-making and law-implementing processes and institutions.[339]

The elements of access to justice[340] were viewed as existing if people, notably the poor and vulnerable, suffering from injustices, have the ability to make their grievances heard, to obtain proper treatment of their grievances either by state or non-state institutions. This, it was considered, would lead to redress of the injustices on the basis of rules or principles of state law, religious law or customary law in accordance with the rule of law.[341] The Rule of Law Access to Justice Scheme which was applied took 'real life problems' and recorded the view of the poor and disadvantaged. The project demonstrated the importance of defining access to justice within a specific context. [342]

The use of Web 2.0 applications represents a specific context of technological innovation which is changing the nature of access in the digital era. As the use of such applications expands, the courts must also ensure there is equal access for the 'tech-savy' and the 'tech-

[337] This project was carried out between 2008-2010 by the Van Vollenhoven Institute (Leiden University) with support from the United Nations Development Program, the World Bank and the Dutch Ministry of Foreign Affairs.

[338] Bedner and Vel, above n 304, 5. The definition of the United National Development Program formed the basis of the definition used by the Access to Justice in Indonesia Project – this was that 'Access to Justice is the ability of people to seek and obtain a remedy through formal or informal institutions of justice, and in conformity with human rights standards'.

[339] Ibid 1.

[340] Ibid 7.

[341] Ibid 7. See also Van Vollenhoven Institute, Universiteit Leiden, *Access to Justice: The concept* (2010) <http://law.leiden.edu/organisation/metajuridica/vvi/research/access-to-justice/access-to-justice/the-concept.html>.

[342] Ibid 10-14.

intimidated'; fair procedures; available funding for technology; and security for the protection of information.[343]

2.3 Innovative technologies – changing access

The most common use of new technologies by courts is the use of sustaining technologies to assist access and to provide legal information. The use of disruptive technologies as a part of the court process is relatively rare, although the term has been used more commonly to describe courts using video links and a variety of computer technologies.[344] There are few virtual courts. The eCourtroom used by the Federal Court of Australia and the Federal Circuit Court of Australia is a virtual court[345] and will be examined in detail in Chapter Five in an analysis of disruptive technologies.

Technological initiatives were supported by the Australian government's report into access to justice[346] as important for providing access to information and supporting the strategic framework.[347] Technologies that have become more common include: videoconferencing; eCourt services, such as efiling; online dispute resolution services, web portals, the National Broadband Network[348] to improve broadband speed, assisting legal assistance services for regional Australia; the use of mobile applications by a variety of government agencies;[349] the use of social media;[350] the use of audio-visual technology;[351] as well as the development of online alternative dispute resolution providers.[352] Australian courts have demonstrated a

[343] Chief Justice Roberts, *2014 Year-End Report on the Federal Judiciary* (Report of the Public Information Office, United States Supreme Court, 31 December 2014) <https://www.supremecourt.gov.publicinfo/year-end/2014year-endreport.pdf>.

[344] Above n 5, see discussion of disruptive and sustaining technologies.

[345] See detailed discussion of virtual and online courts in Chapter 5 of this thesis, 179-224.

[346] Access to Justice Taskforce, 'A Strategic Framework for Access to Justice in the Federal Civil Justice System', Report to the Attorney-General's Department, Australian Government, September 2009), Chapter 6, 'Information about the law' <https://www.ag.gov.au/LegalSystem/Pages/Accesstojustice.aspx> 77-86.

[347] Ibid. Recommendation 6.8 of this Report was that '[g]reater emphasis should be placed on the opportunities that using new technologies can afford to improve the efficiency and scope of service delivery on a cost-effective basis', 84.

[348] The National Broadband Network is an open-access data network being developed in Australia to provide high capacity transmission and infrastructure for internet access: <http://www.nbnco.com.au>

[349] Court lists in Victoria can be accessed by downloading The Daily List app from the Victorian Bar website (<http://www.vicbar.com.au>). The court lists available include those from: the Magistrates' Courts of Victoria; the County Court of Victoria; the Supreme Court of Victoria and the Victorian Court of Appeal.

[350] Links to Facebook and Twitter can be found from the Supreme Court of Victoria's website <http://www.supremecourt.vic.gov.au>

[351] Audio-visual recordings of Full Court hearings of the High Court of Australia are made available on the court's website: <http://www.hcourt.gov.au> to improve public access to its hearings. The audio-visual recording is usually available within a business day after the Court has finished sitting.

[352] Online dispute resolution of family court matters is provided by FamilyResolve which connects parents and partners with mediators using webcam-enabled online dispute resolution. The aim is to provide a faster, more

willingness to 'make judicial procedure and decisions more accessible and understandable to the public'[353] and by using technology proactively, broadcasting judgment summaries and sentencing remarks to provide greater access to the courts.[354] By 2014 it was reported that there had been considerable investments in court technologies, although there was considerable differences in availability and quality in some jurisdictions.[355] Case management software, efiling and electronic trial technologies were identified as contributing most to cost savings and access to justice.

Another example of digital tools delivering information and open access is software such as A2J Author,[356] a web-based interface, which was created to deliver access to justice for self-represented litigants by assisting them to complete and print court documents that can they be filed in the court system. It provides guided interactive interviews[357] for court forms and is available through court and state wide websites. The New York State Courts Access to Justice Program has created a program accessible in English, Spanish and French. Videos are provided for self-represented litigants to assist them in understanding the programs. The A2J Author has developed a YouTube channel with up to date information on training promoted on Twitter. Staudt[358] found that the potential transformational changes these technologies could offer included: public access to document assembly; customer-friendly Web-mediated direct services to clients; deep integration of legal aid agencies' internal document and case management systems with customer-facing systems delivered over the internet; wider coordination of legal aid agencies' internal systems with the case and document management systems of other agencies and direct internet connection between legal aid case and document management systems and the administrative agencies and courts delivering benefits and deciding matters.[359] Staudt considered that the success of such systems has led to 'an enthusiasm for using technology to deliver more effective and less expensive legal information and to provide services to low-income clients of legal aid'.[360]

cost effective and efficient resolution of disputes which is also more flexible and available to interstate or internationally based parties at convenient hours <http://familyresolve.com.au>.

[353] P Keyzer, J Johnston and M Pearson (eds) *The Courts and the Media: Challenges in the Era of Digital and Social Media* (Halstead Press, 2012) 79.

[354] Ibid 76.

[355] Productivity Commission, Inquiry Report No 72, *Access to Justice Arrangements ,* Volume 1, Chapter 17, 'Courts – technology, specialization and governance' (5 September 2014), 573.

[356] Access to Justice Author, above n 46. This was discussed in 1.2.1 in relation to the innovative developments of Web 2.0.

[357] <http://www.kentlaw.edu/cajt/A2JAuthor.html>.

[358] Staudt, above n 39, 1117.

[359] Ibid 1144-1145.

[360] Ibid 1144.

In the US, every state and jurisdiction has been reported as having legal informational websites which can be accessed through the Law Help website,[361] however, there is not yet a single user portal and there are many challenges for the future, including improving multi-lingual access and making more content available for mobile platforms. These mobile platforms would be targeted for improvement because most often low income people access the internet this way. The creation of a Center on Mobile Access to Justice Technology was proposed to develop such applications as court reminders by phone which would link to preparation tools and 'movement analyzing algorithms to identify domestic violence incidents'.[362]

A comprehensive report by the Harvard's Berkman Center for Internet & Society evaluated how the use of technology could facilitate access to justice in the Massachusetts Trial Court. The report identified four categories of technology which could be most useful to self-represented litigants. These categories include: a 'clear, simple, well-organized and up-to-date Court web site'; the easy completion of court forms online; case management and e-filing systems; and individualised human assistance. It was considered that the website should target the proper audience and be an effective initial contact point'; it should be clear, easy to navigate; be multilingual; with multimedia available; and have comprehensive information about all the courts including accessible primary legal materials, detailed procedural guides, easy-to-use forms, simple step-by-step guidance, information on limited assistance representation, and information about finding lawyers. An automated electronic guided interview was thought to be technology that could assist self-represented litigants with complicated tasks, using software such as A2J Author.[363] The report contained detailed recommendation about how the technology should be deployed, particularly to make access to computers, e-filing and other technologies possible for self-represented litigants.[364]

[361] The Law Help website was created in 2001 for people on low incomes and for legal organisations that assist them. It is maintained by Pro Bono Net (a national nonprofit organization based in New York City and San Francisco) and hundreds of nonprofit legal aid, pro bono, court-based programs and libraries across the US <http://www.LawHelp.org>.

[362] Richard Zorza, 'Review of the Status and Potential of Access to Justice Technology in the United States of America' (June 2013) paper presented to the meeting of the International Legal Aid Group <http://www.zorza.net> 10.

[363] Access to Justice Author, A2J, above n 46.

[364] Cyberlaw Clinic, *Best Practices in the Use of Technology to Facilitate Access to Justice Initiatives* (Preliminary Report, Berkman Center for Internet & Society at Harvard University, July 30, 2010). This report was prepared for the Hon Dina E Fein, First Justice, Housing Court Department, Western Division and Special Advisor to the Trial Court for Access to Justice Initiatives <https://cyber.harvard.edu/publications/2010/Best_Practices_Technology_Access_to_Justice>.

Grainger[365] recommended effective strategies which use technology in 'innovative ways' to enhance access to justice in Australia, especially for litigants in person. Grainger's research focussed on strategies adopted in the US and the UK where she found that the most effective strategies in the US encourage self-help and the provision of high quality, 'detailed information about the law and courts' practices and procedures'. This enabled more people to be assisted with limited resources. Her recommendations for Australia included the use of a strategic plan for litigants in person, the provision of abundant information, access to the internet at courts and tribunals, the use of text message technology, smartphone applications, interactive self-completing (or do-it-yourself) forms, interactive web-based question and answer forums, video conferencing technologies, community legal education, electronic files and self-help centres.

The widespread use of mobile technology, particularly the use of smart phones and Web 2.0 applications on mobile devices has provided new opportunities for the provision of legal services.[366] Mobile devices and networks have been seen as the main way of accessing information and will offer new opportunities for the provision of legal services in the future.[367] Providing security for personal information, particularly with court documents containing personal and confidential information will be more difficult with the development of mobile access.[368] The use of mobile devices for access to justice is an area for on-going future research.

The transformation of paper-based court documents to digital files, particularly the use of e-filing led Cabral and Clarke to advocate for 'the creation of an application ecosystem through the adoption of open technical standards for e-filing' to ensure there is 'universal access to and interoperability between courts and legal aid providers'.[369] The development of an appropriate triage system was seen as vitally important for the provision of full access to legal services, although, its application may prove difficult because the system needs to protect litigant

[365] Julie Grainger, *Litigants in Person in the Civil Justice System – learning from NZ, the US and the UK* (Report prepared for The Winston Churchill Memorial Trust of Australia, 1 November 2013).
[366] Abhijeet Chavan, 'Mobile Strategies for Legal Services' in James E Cabral et al, Using Technology to Enhance Access to Justice' (2012) 26 *Harvard Journal of Law & Technology* 241-324, 267-278.
[367] Ibid.
[368] Bonnie Rose Hough, 'Let's Not Make it Worse: Issues to Consider in Adopting New Technologies' 256 - 266 in James E Cabral et al, Using Technology to Enhance Access to Justice' (2012) 26 *Harvard Journal of Law & Technology* (2012) 26 *Harvard Journal of Law & Technology* 241-324.
[369] James E Cabral and Thomas M Clarke, 'Using Technology to Enhance Access to Justice' in James E Cabral et al, Using Technology to Enhance Access to Justice' (2012) 26 *Harvard Journal of Law & Technology* 241-324, (2012) 26 *Harvard Journal of Law & Technology* 278-292. The technical triage system proposed was one based on algorithms which would have the capacity to find the underlying patterns in data.

privacy. [370] Hough and Zorza considered that people must be able to control the flow of information and be provided with the tools necessary to assess the risks and prevent their personal information reaching 'certain end users'. This was seen as particularly relevant in areas of child support and domestic violence where confidentiality is important.

The development of supportive digital tools has developed rapidly over the past ten years with an accompanying promise to improve efficiency, to lower costs and provide greater access to courts for anyone with internet access, whether by home or office computers or by mobile devices. The extent to which new technologies will provide assistance with legal processes is less clear. The important factor is for access and open justice to be complementary, so that a just resolution of disputes in courts is not hampered by technologies which are unable to protect the integrity of the legal process.

The use of electronic filing, while not yet widespread, has changed the nature of the availability of documents. With the 'move towards fully electronic courts and electronic court records … countervailing interests and challenges' are being faced by the courts in particular a demand to 'enhance public rights of access to court records'.[371] The increased demand and public expectation for improved access and re-use of public sector information has followed the 'growing capacity of networked digital information technologies to process and visualise large amounts of information in a timely, efficient and user driver manner'.[372] In particular, this has been encouraged by the development of Government 2.0 which encompasses the use of tools facilitating collaboration, efficient government and accountability. The improvement in access to public sector information and its use has been acknowledged as 'of major importance for all economies'.[373] However, it has been acknowledged that openness applies to a 'different extent to different categories of information and content', depending on such issues as: legal requirements, privacy, confidentiality, national security, human rights and freedom of information.[374]

[370] Bonnie Rose Hough and Richard Zorza, 'Tech-Supported Triage: The Key to Maximizing Effectiveness and Access - Using Technology to Enhance Access to Justice' (2012) in James E Cabral et al, Using Technology to Enhance Access to Justice' (2012) 26 *Harvard Journal of Law & Technology* 26 *Harvard Journal of Law & Technology* 241-324, 292-304.

[371] Judith Bellis, 'Public access to court records in Australia: An international comparative perspective and some proposals for reform' (2010) 19 *Journal of Judicial Administration* 197-231, 200.

[372] Brian Fitzgerald (ed), 'Access to and Re-use of Public Sector Information', Vol 1, Chapter One, *Access to Public Sector Information: Law, Technology & Policy* (Sydney University Press, 2010) vii.

[373] Graham Vickery, 'Foreword', in Brian Fitzgerald (ed), Vol 2, *Access to Public Sector Information: Law, Technology & Policy* Vol 2 (Sydney University Press, 2010) vii.

[374] Ibid.

Paradoxically, the 'substantial diminutions in the use of orality in court'[375] and new procedures introduced to accommodate the changes in technology have altered what is meant by documents being available to the public as well as the nature of public information within the courtroom. Procedures that have changed include: counsel handing up documents in court or witnesses providing evidence in chief by statements or affidavits read silently by the judge and counsel before cross-examination, so that they are no longer read aloud in court. Also in electronic trials, vast number of documents are tendered and accessed directly from computers, inaccessible by members of the public. These procedures have been adopted to improve efficiency and economy however they have impacted on the nature of a public trial. The practice of evidence being received by the courts but not read in open court has been alleged to have the potential 'side effect of making the proceedings less intelligible to the press and the public'.[376]

Procedures adopted for efficiency such as the filing of written submissions of evidence in chief by affidavit, has been criticised as making it difficult for members of the public to understand proceedings and of reducing the opportunity for public scrutiny.[377] These procedures have been seen as failing to 'take account of the public interest in the open administration of justice'[378] and has been an 'unintended consequence of judicial procedures adopted in the interests of the efficient administration of justice'.[379] The remedy was seen to lie with the courts to provide the public with reasonable access to such documents[380] to remedy the unintended consequence of having court procedures that are no longer truly open.[381]

Lord Bingham considered that in resolving the 'tension between efficient justice and open justice' the court should 'give appropriate weight to both efficiency and openness of justice'. It was considered that while there were reasons for improving efficiency and protecting private information, 'the important private rights of the litigant must command continuing respect. But so too must the no less important value that justice is administered in public and

[375] Justice Steven Rares, 'How the implied Constitutional Freedom of Communication on Government and Political Matter may require the Development of the Development of the Principles of Open Justice', Judicial Conference of Australia Colloquium 2007, Sydney, [59]-[61].
[376] *R (Guardian News & Media Ltd) v City of Westminster Magistrates Court* [2012] WLR 1343, 1367.
[377] Ernst Willheim, 'Are Our Courts Truly Open?' (2002) 13 *Public Law Review* 191-204, 203-204.
[378] Ibid, 204.
[379] Ibid.
[380] Ibid 204.
[381] Ibid 191.

is the subject of proper public scrutiny'.[382] The challenge of resolving this tension has become more difficult in the digital era.

2.4 Digital access to justice

2.4.1 Introduction: defining digital access

Using Web 2.0 applications can provide digital access to justice and this has led to the emergence of different definitions. One of the first definition of access to justice to be formulated with the technologies in mind was that adopted by the Washington State justice system[383] in Access to Justice Technology Principles. This refers to:

> The meaningful opportunity, directly or through other persons: (1) to assert a claim or defense and to create, enforce, modify, or discharge a legal obligation in any forum: (2) to acquire the procedural or other information necessary (a) to assert a claim or defense, or (b) to create, enforce, modify, or discharge an obligation in any forum, or (c) to otherwise improve the likelihood of a just result; (3) to participate in the conduct of proceedings as witness or juror; and (4) to acquire information about the activities of courts or other dispute resolution bodies. Furthermore, access to justice requires a just process, which includes, among other things, timeliness and affordability. A just process also has 'transparency', which means that the system allows the public to see not just the outside but through to the inside of the justice system, its rules and standards, procedures and processes, and its other operational characteristics and patterns so as to evaluate all aspects of its operations, particularly its fairness, effectiveness, and efficiency.[384]

The Principles provide a broad definition of 'technology'. It includes: 'all electronic means of communication and transmission and all mechanisms and means used for the production, storage, retrieval, aggregation, transmission, communication, dissemination, interpretation, presentation, or application of information'.[385] The Principles state the governing values which are to be used to guide the use of technology in the State's justice system. Access to justice is recognized as a 'fundamental right'. An Access to Justice Board was established to protect this right. The Principles require the decision makers in the justice system to consider 'access to justice' when they plan or implement technology so that technology enhances rather than reduces access to justice. The Principles were designed to be practical and effective for the

[382] *SmithKline Becham Biologicals SA v Connaught Laboratories Inc* [1999] EWCA Civ 1791.

[383] Access to Justice Principles are available on the Access to Justice Website: <http://www.atjweb.org>. They were 'developed by the Access to Justice Board to ensure that technology enhances rather than diminishes access to and the quality of justice for all persons in Washington State'. The website contains resources to assist with the implementation of the Principles. The Access to Justice Board is a partner of EdLab Group, Communities Connect Network <http://www.edlabroup.org> This Network is a statewide coalition of public and private organizations to ensure 'digital inclusion' and all individuals have access and the skills to use the internet and information technologies.

[384] Ibid. Washington State Access to Justice Technology Principles were adopted by the Washington State Supreme Court, December 3, 2004. The Preamble provides a definition of access to justice, 2.

[385] Ibid 4.

'workers in and users of the justice system'. They fit within Lord Neuberger's requirements for access to justice by making courts accessible, providing effective procedures for getting cases before the courts and by providing effective legal processes.

These Principles recognised the 'dual responsibility' of the justice system to be open and protect personal privacy [386]. They also recognised that technology can 'create or magnify conflict between these values', so they recommended that technology should be designed to meet both responsibilities. There is an understanding that openness and privacy are not necessarily in conflict when technology is designed to protect these values. When there is a conflict, the Principles require the decision makers to balance both openness and privacy and their underlying objectives, assessing the potential effects of technology.

Digital access as a pathway to justice has become possible over the past ten years in an age of considerable technological maturity, particularly with the use of the innovative applications of Web 2.0. They are presenting a transformed paradigm for access to justice. The courts have been become involved in the complex contemporary media landscape and have 'both *sought out* visibility and had visibility imposed on them' in the new digital era.[387] Such a digital pathway has been based on digital legal platforms linking claimants to the courts, offering options and solutions with enhanced legal services. As well, mobile technology and interactive devices complement computer platforms by facilitation mobile internet access. This digital pathway has not developing rapidly, although, there has been substantial success in the development and application of new technologies to legal processes in countries such as the US, the UK and Australia over the past ten years.

As the Chief Justice of the United States Supreme Court has reported:

> the courts will often choose to be late to the harvest of American ingenuity. **Courts are simply different in important respects when it comes to adopting technology**, including information technology … the courts are neutral arbiters of concrete disputes that rely on parties with genuine grievances to initiate the process and frame the issues for decision. The courts' passive and circumscribed role directly affects how courts deploy information technology. The courts understandable focus on those innovations that, first and foremost advance their primary goal of fairly and efficiently adjudicating cases through the application of law. [388]
> (emphasis added)

[386] Ibid.

[387] Jane Johnston, 'Courts' new visibility 2.0', in Patrick Keyzer, Jane Johnston and Mark Pearson (eds), *The Courts and the Media: Challenges in the era of digital and social media* (Halstead Press, 2012) 41-54.

[388] Roberts, Chief Justice, above n 343, 3-4.

In referring to the passive and relatively restricted role in the use of information technology, the Chief Justice emphasised the importance for courts of prudence and discretion in the adoption of technologies which may impact on the adjudication of cases.

Reiling[389] predicted that 'online transaction will become the norm' because this will be what the public will expect. Reiling distinguished digital access from general information technology as 'two-way communication', including e-filing and full electronic case processing. She found that the use of such applications by the courts in 2009 was rare but would increase with time and the demand for self-representation.[390] Just as the last 15 years had seen a much greater demand for digital access and a greater availability of such services. She did not consider that it was necessary to have sophisticated systems for self-represented litigants because simple forms of access would be sufficient and could be developed in stages from one-sided information delivery, to downloadable forms and finally 'full transaction: case handling, decision and delivery'.[391] Zorza found that the 'substantial majority of technology innovation has focused on assistance to the self-represented'[392] litigant because so little of the demand for access to the civil legal system has been met by traditional processes. Ribadeneyra[393] assessed the capacity of web-based technologies to deliver legal services for low income litigants in the US, including: filing, web services, OSNs and online document assembly, however, concluded that more needed to be done to improve accessibility and usability.

Reiling found that '[a]ccess to legal information is an important factor in resolving problems, assisting in resolving issues out of court and improving integrity by providing transparency'.[394] This information and knowledge required to solve justiciable problems Reiling considered could be found on the internet.[395] She discussed the support information technology could offer in enabling parties to settle and stay out of court or alternatively to resolve their disputes in the best way possible. Reiling referred to the work of Galanter and the differing needs of

[389] Reiling, above n 229, 269.
[390] Ibid 268.
[391] Ibid 268-269.
[392] Richard Zorza, 'Review of the Status and Potential of Access to Justice Technology in the United States of America' (Paper presented at the International Legal Aid Group conference, The Hague, 12-14 June 2013) <http://www.internationallegalaidgroup.org/index.php/papers-publications/conference-papers-reports/category/7-conference-papers> 2.
[393] James E Cabral et al, 'Using Technology to Enhance Access to Justice' (2012) 26 *Harvard Journal of Law & Technology* 246.
[394] Reiling, above n 229, 263.
[395] Ibid 183.

those who are new to court processes and parties who are experienced.[396] Reiling considered that information technology could assist, not only by providing 'correct, adequate information' to 'enhance the procedural position of the court users', but also by giving those who are new to court processes a better opportunity for a 'just and fair outcome' of their matter. The recommendations were for the use of a 'proactive, demand oriented and differentiated information service', together with '[m]ulti-channel information' and reference to information on the court website, information from other sources and unified and simplified court access.[397]

The digital pathway was viewed as supplementary to current procedures not a substitute for them and supportive of access. Reiling concluded that some form of 'human help should always be available' when the more advanced interaction is offered by the courts. This would ensure that access to justice would be improved by the provision of 'a realistic understanding of their processes'. The study found that information whether of the 'information push' variety or interactive forms of technology could be used to reduce disadvantages that people who only litigate once face and to assist self-represented litigants.[398] It could also 'actively contribute to improved access to justice' in the field of public trust by 'ensuring correct information about their processes'.[399]

The design of 'an accessible, technology-driven justice system'[400] in the US was also viewed by Small et al as not a 'replacement legal system' but a technological information system which would assist people to solve most of their own legal issues. The idea was to envisage an idealised civil justice system that could take advantage of all technological opportunities making the justice system function more efficiently and enhance the value of outcomes. Technology was seen as a tool, providing an information system that would allow people to solve most of their own legal issues with only a small number requiring adjudication.

[396] March Galanter, 'Why the "haves" Come Out Ahead: Speculations on the Limits of Legal Change' (1974) 9 *Law and Society Review* 95-160.
[397] Reiling, above n 240, 192.
[398] Ibid 195-207.
[399] Ibid 195-207.
[400] T W Small, Robert Boiko and Richard Zorza, 'Designing an Accessible, Technology-Driven Justice System: An Exercise in Testing the Access to Justice Technology Bill of Rights' (2004) 79 *Washington Law Review* 223-250. This article described a justice system designed speculatively for twenty years in the future using technology available in 2004 and a system that maintained 'core values' such as fairness, openness and availability to all people.

However, digital access to justice can be viewed as more than a technologically augmented solution to litigation but an alternative pathway for the settlement of legal disputes, supporting the administration of justice by the use of virtual courtrooms, OSNs and the applications of Web 2.0 to enhance access to justice.

2.4.2 Transparency and open courts

The development of technologies such as virtual courts has raised fundamental questions about what characteristics define a court, particularly what openness and transparency mean in the digital era. Stepniak has examined whether 'the implementation of the principle of open justice needs to be reconsidered'.[401] He suggested that the televising of court proceedings should be allowed 'principally because open justice requires that the administration of justice be conducted in open courts unless it can be established that justice cannot otherwise be done'.[402] The benefits found included providing the opportunity for all members of society to observe court proceedings, the possibility that the 'dignity and decorum' of parties may be enhanced and the possibility that it may also reduce the physical disruption.[403]

The recommendation that televising court proceedings would improve accessibility was limited by the suggestion that 'clear and firmly enforced set of guidelines' would be essential which would need to be flexible and 'protect the independence of the judiciary'.[404] In his assessment of the application of technological advancement to courts, particularly the use of audio-visual technology, Stephniak argued that to insist that there should be 'substantiated absence of effects as a prerequisite to audio-visual recording and broadcast of court proceedings' would not be compatible with the principles of open justice.

The important issue for Stepniak in determining whether such coverage should be permitted and how it should be regulated is considering whether it is 'a medium of public information capable of enhancing public access and understanding of judicial proceedings'.[405] The recording and broadcasting of court proceedings in Australia, New Zealand, the UK, US and

[401] Daniel Stepniak 'Technology and Public Access to Audio-Visual Coverage and Recordings of Court Proceedings: Implications for Common Law Jurisdictions'. (2004) 12 *William & Mary Bill of Rights Journal* 791-823, 792.
[402] Daniel Stepniak, 'Why Shouldn't Australian Court Proceedings be Televised?' (1994) 17 *UNSW Law Journal* 345-382, 350.
[403] Ibid, 351.
[404] Daniel Stepniak, *Audio-Visual Coverage of Courts* (Cambridge University Press, 2008) 381.
[405] Ibid 7.

Canada suggested to Stepniak that appropriate regulations and controls could minimise, if not eradicate, the potentially detrimental impact of 'cameras in courts'.

Although for different and contrasting reasons to Stepniak, Jaconelli in his assessment of open justice also considered that it was time for a reassessment of the public trial because modern technology, while making it possible to convey trial information to a 'worldwide audience' the 'interposition of any medium between the *personae* of the trial and the rest of the world diminishes the effect of open justice'. He considered it may falsify the 'reality of the courtroom'[406] by placing technological barriers between the accused and witnesses. However, in assessing technology at the beginning of the 21st century, Jaconelli refers to the lack of scientifically reliable data on the performance of the *personae* of the trial under different conditions, particularly in relation to the question of televised coverage of trials, particularly the difficulty in conducting controlled experiments.[407] These observations were made before the technological advances of the past decade. Lederer, however, viewed the virtual courtroom as the 'eventual destination' where travel is eliminated, document transmission and evidence presentation is efficient,[408] and one that is 'truly public if any member of the public could "log in" to a trial'.[409]

Open access to court documents and the application of the principle of open justice has been considered by the courts often, particularly in cases of public interest where journalists have sought access. In *R (Guardian News & Media Ltd) v City of Westminster Magistrates Court* [410] the Court concluded that open justice is a constitutional principle to be found in the common law, vital to the rule of law and '[w]hile the broad principle and its objective are unquestionable, its practical application may need reconsideration from time to time to take account of changes

[406] Joseph Jaconelli, *Open Justice: A Critique of the Public Trial* (Oxford University Press, 2002) 354.
[407] Ibid 353-354.
[408] Frederic I Lederer, 'The Road to the Virtual Courtroom? A Consideration of Today's – and Tomorrow's – High Technology Courtrooms' 1999) 50 *South Carolina Law Review* 799-844, 844.
[409] Ibid 843.
[410] *R (Guardian News & Media Ltd) v City of Westminster Magistrates Court* [2012] EWCA Civ 420 [69]. In this case, the United States Government sought extradition of two British citizens on corruption charges under the *Extradition Act* (2003). They were alleged to have been involved in the bribery of Nigerian Officials by a subsidiary of a well-known US company. Journalists for the Guardian had attended part of the hearing where council referred to certain documents, including affidavits, witness statements and correspondence but they were not read out in detail. The application to the District Court failed and the Divisional Court of the Queen's Bench Division dismissed the claim and the appeal at common law and under article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms. The Court of Appeal held that the claimant had a serious journalistic purpose in seeking access to the documents concerned with international corruption and extradition and the public should be informed.

in the way that society and the courts work'.[411] In undertaking a fact-specific exercise in proportionality the court would need to evaluate the open justice principle, the potential value of the material and any risk of harm which access to the documents may cause.[412]

While technology provides the means to enable open access to all court documents other factors mitigate against unrestricted access. Electronic court records made available on the internet were seen by Eltis as having the potential to affront 'the very access to justice that digital files were meant to promote' particularly when personal information is inadvertently disclosed 'in ways not anticipated by existing rules'.[413] She distinguished between the past and present with the 'audience of incalculable numbers' on the internet which provides the 'new conception of "accessibility"'.[414] Eltis referred to 'unrestrained disclosure' with the subsequent loss of control over the courts' own records, which can 'chill access to the courts' such that "access" may no longer serve the rationales of openness and accountability and instead undermines the very entry to justice it was intended to foster'.[415] The solution suggested was the construction of privacy to be found in the civil law which she considered 'better able to protect individual privacy in intangible spaces (such as cyberspace) due to the interpretation of privacy 'as a zone of intimacy delineated not by space or ownership but by the basic needs of personhood'.[416]

Lord Diplock delineated the boundaries of open justice in relation to the administration of justice:

> The application of this principle of open justice has two aspects: as respects proceedings in the court itself it requires that they should be held in open court to which the press and public are admitted and that, in criminal cases at any rate, all evidence communicated to the court is communicated publicly. As respects the publication to a wider public of fair and accurate reports of proceedings that have taken place in court the principle requires that nothing should be done to discourage this.
>
> However, since the purpose of the general rule is to serve the ends of justice it may be necessary to depart from it where the nature or circumstances of the particular proceeding are such that the application of the general rule in its entirety would frustrate or render impracticable the administration of justice or would damage some other public interest for whose protection Parliament has made some statutory derogation from the rule. Apart from statutory exceptions, however, where a court in the exercise of its inherent power to control the conduct of proceedings before it departs in any way from the general rule, the

[411] *R (Guardian News and Media Ltd) v City of Westminster Magistrates' Court* [2012]WLR 1343, 1349, Toulson LJ.
[412] *R (Guardian News and Media Ltd) v City of Westminster Magistrates' Court* [2012]WLR 1343, 1368.
[413] Karen Eltis, 'The Judicial System in the Digital Age: Revisiting the Relationship between Privacy and Accessibility in the Cyber Context' (2011) 56 *McGill Law Journal* 289-316, 291.
[414] Ibid 295.
[415] Ibid 302.
[416] Ibid 314. See also analysis in Chapter Three of this thesis.

> departure is justified to the extent and to no more than the extent that the court reasonably believes it to be necessary in order to serve the ends of justice.[417]

This emphasised two main aspects of open justice, the proceedings themselves and the report of proceedings. The openness of reporting proceedings was also discussed by Sir Gerard Brennan as an important element of the judicial method. He considered that, 'subject to narrow exceptions, every word that is uttered from the opening sentence of a case to the closing words of an appellate judgment be open to scrutiny. Nothing must be hidden'.[418] He considered that popular respect for the administration of justice would be something earned by 'steady and manifest adherence to the judicial method'.[419]

Open justice has been referred to as 'one of the most pervasive axioms of the administration of common law systems'[420] which dictates that judicial proceedings 'must be conducted in an open court to which the public and the press have access'.[421] It has also been described as meaning 'unfettered public access to proceedings' in the courts. [422] The terms 'open', 'justice' and 'access' are linked by their interaction with one another in that openness appears to be a prerequisite of access and without access there is no path to justice.

The principle of open justice is a common law principle, according to Lord Neuberger, stretching back into the earliest period of common law.[423] A principle important because of 'the role it plays in supporting the rule of law'[424] and guarding against repression.[425] The two fundamental problems Lord Neuberger detected in relation to justice he considered could be 'summarised in one word, accessibility: accessibility to the law and accessibility to the

[417] *Attorney-General v Leveller Magazine* [1979] AC 450. In this the case the Court considered whether there had been contempt of court by publishers of certain magazines by publishing the name of a witness. It was held that where a court had made a ruling to prevent publication and someone, knowing the purpose of the ruling, frustrated this by such publication, the act might be considered contempt of court in interfering with the due administration of justice. However, in the present case it was held that intended effect of the ruling that the witness' name not be published had been abandoned by the witnesses' disclosure in evidence which had not been prevented by the court or the prosecution. Therefore there had been no interference with the due administration of justice in the publication of the witness' name.

[418] Ibid 91.

[419] Sir Gerard Brennan, 'Why be a Judge?' (1996) 14 *Australian Bar Review* 89-96, 90.

[420] James Spigelman, former Chief Justice of New South Wales, 'Seen to be Done: The Principle of Open Justice' (Keynote Address presented at the 31st Australian Legal Convention, Canberra, 9 October 1999) 3.

[421] Ibid.

[422] Wayne Martin, Chief Justice, 'Improving Access to Justice: The Role of the Media' (Paper presented to the School of Media, Culture and Creative Arts, Curtin University, 15 October 2009) 2.

[423] Lord Neuberger, 'Open justice unbound?' (2011) 10 *The Judicial Review* 260.

[424] Ibid.

[425] Ibid 275.

courts'.[426] At common law exceptions to the principle of open justice were recognised in *Scott v Scott*[427] where Viscount Haldine LC explained that the exceptions are 'the outcome of a yet more fundamental principle that the chief object of Courts of justice must be to secure that justice is done'. The principle however can only be displaced when it is necessary for justice to be achieved and not out of convenience.

Lord Denning recognised that over time there have been attempts to 'whittle down' the principle of publicity and open justice, however, considered:

> we must hold fast to the principle that every case must be heard and determined in open court. It must not take place behind locked doors. Every member of the public must be entitled to report in the public press all that he has seen and heard.[428]

Australian courts have followed this principle of open justice which can be seen in the decision in *Scott v Scott*. Also in *Dickason v Dickason* [429] an application to hear the matter *in camera* was refused because it was held that the Court had no inherent power to exclude the public unless there was a clear statutory provision to the contrary. As Justice Gibbs stated in *McPherson v McPherson*[430] concerning the virtue of the rule requiring proceedings to be public and open:

> The fact that courts of law are held openly and not in secret … distinguishes their activities from those of administrative officials, for publicity is the authentic hall-mark of judicial as distinct from administrative procedure.[431]

His Honour considered that open courts exposed proceedings 'to public and professional scrutiny and criticism, without which abuses may flourish undetected'[432]. This openness and access was important because it assisted in maintaining confidence in the integrity and independence of the courts.

---

[426] Lord Neuberger, above n 297, 3.

[427] *Scott v Scott* [1913] AC 473. In this case Lord Shaw found that it is 'a sound and very sacred part of the constitution of the country and administration of justice'.

[428] Sir Alfred Denning, *The Road to Justice* (Stevens & Sons, 1955) 64.

[429] *Dickason v Dickason* (1913) 17 CLR 50. In this case the petitioner applied to the High Court for the appeal to be heard in camera. The respondent consented to the application being granted however it was held at 51 that the application could not be granted because the 'matter appears to be concluded by the judgments of the Lords in *Scott v Scott*'.

[430] *McPherson v McPherson* [1936] AC 177.

[431] *McPherson v McPherson* [1936] AC 177, 200.

[432] *McPherson v McPherson* [1936] AC 177, 200.

The constitutional significance of the open justice principle has been considered by the High Court of Australia in a number of cases, particularly in relation to the important attributes of a court. As Justice Gibbs stated in *Russell v Russell*:

> The fact that courts of law are held openly and not in secret is an essential aspect of their character. It distinguishes their activities from those of administrative officials … In requiring them to sit in closed court in all cases – even proceedings for contempt – the Parliament has attempted to obliterate one of their most important attributes. This it cannot do. [433]

Chief Justice Barwick in considering s 97(1) of the *Family Law Act 1975* (Cth) and the requirement that all proceedings in the Family Court, or in another court when exercising jurisdiction under this Act, were be heard in closed court, held that this section was invalid 'so far as it purports to require the State court to be closed to the public, when invested jurisdiction under the Act is being exercised'. His Honour considered that this subsection purported 'to take from the State Court any discretion to exclude the public in certain particular circumstances' and required the courts to exercised its invested jurisdiction 'behind closed doors'. This decision was supported by the High Court in *Hogan v Hinch*[434] in which Chief Justice French discussed the open-court principle in detail.[435] His Honour found that the principle was 'a means to an end, and not an end in itself'. It is not an absolute principle, despite it being an essential characteristic of courts. It remains a principle important to achieve justice rather than simply a characteristic of the courts.

There have always been limits placed on open courts. Jaconelli cautioned that 'there exists a golden mean that lies between the one extreme of secrecy and the other extreme of excessive exposure of judicial proceedings to the public gaze'.[436] In deconstructing the concept of 'open justice', Jaconelli identified six 'presumptive elements': the first, provision of adequate facilities to enable members of the public and the press to attend; the second, the right of those in attendance to report the proceedings; the third, the availability of court documents for

[433] *Russell v Russell* (1976) 134 CLR 495. In this case parental rights and the custody and guardianship of infants were considered by the High Court as well at the regulation of practice and procedure of State courts exercising jurisdiction under the *Family Law Act 1975* (Cth).

[434] *Hogan v Hinch* (2011) 243 CLR 506. In this case s 42 of the *Serious Sex Offenders Monitoring Act 2005* (Vic) and the provision that, if the court was satisfied that it was in the public interest, they might order that any information that could identify a person or offender who had appeared or given evidence must not be published. Derryn Hinch, a radio broadcaster, responsible for a website at that time "HINCH.net". He was charged with contravening suppression order. He raised a constitutional challenge to the validity of s 42 and the basis that the orders represented an infringement upon the open-court principle. It was held that s 42 was not invalid on the ground raised.

[435] *Hogan v Hinch* (2011) 243 CLR 506, [20]-[27].

[436] Jaconelli, above n 406, 1.

inspection; the fourth, the open availability of the names of the personnel of the trial; the fifth, the trial taking place in the presence of the accused, and finally the right of the accused to confront the accusers.[437] Jaconelli[438] identified place, time and function as the main elements of trials in the more traditional sense, although he found that what constitutes a 'court' has not always been clear, in particular, he considered that 'no trial depends for its validity on its having been staged in a purpose-built courtroom'.[439]

In regard to place, most trials at the beginning of the 21st century have been held in a 'purpose-built court'[440] with familiar physical layout and spatial elements,[441] although there have often been provisions for makeshift courtrooms and scene viewing.[442] Examples of this include the hearing of native title cases in the Federal Court in desert locations. By 2001 technology had made a significant impact on the nature of a courtroom in the hearing of *De Rose v State of South Australia*[443] by Justice O'Loughlin of the Federal Court of Australia. The first mobile electronic courtroom[444] was developed to enable the native title trial to be conducted in several remote locations using tents, laptop computers, screen displays of evidence and wireless networks and servers. A small outpost 470 km south of Alice Springs being used as the residence for technology, court staff and the Judge for the six week trial. This was a pilot project and formed part of the Federal Court's e-court development to deliver access to justice and required the court to define the meaning of electronic trial.

As Jaconelli has described, courts usually sit at standard times,[445] although this is now no longer necessary. Special courts, such as the drug night court program of Cook County Circuit Court in the US,[446] expanded standard court times, to relieve a backlog of cases and in Singapore[447] to hear minor offences and to make is possible for the working public to attend.

[437] Ibid 2-4.
[438] Ibid.
[439] Ibid 11.
[440] Ibid.
[441] Ibid 13.
[442] Allison Stanfield and Louise Anderson, 'The Federal Court goes bush' 22 June 2001 *Lawyers Weekly* 16 – 17.
[443] *De Rose v South Australia* [2002] FCA 1342;
[444] Stanfield and Anderson, above n 442.
[445] Jaconelli, above n 406, 13.
[446] The Cook County Drug Court Treatment Program was established in 1998 to address drug and alcohol abuse in Illinois and offers an alternative sentencing approach for non-violent offenders. <http://www.cookcountycourt.org>.
[447] The Night Courts were established in 1992 to deal with the high volume of regulatory and traffic offences in State Courts <http://www.statecourts.gov.sg>.

Virtual courts, such as eCourtroom can be opened on one day and closed several days later, depending on the urgency of the matter.[448]

Whether a court should be open to the public can be analysed by function. This refers to the nature of the work undertaken by the court. It has been reasoned that if the function is judicial rather than administrative the presumption that the proceedings should be open follows. Jaconelli concluded:

> The concept of the 'judicial' function is simply too vague to act as a reliable guide to the procedures which should, and should not, be open to public access. Many of the procedural contexts that lie outside the trial proper have simply not formed the subject of challenge by those who have a strong interest in asserting public or press access. Long established practice appears to be decisive of the issue of whether certain procedures should be open or closed. In many situations, even if the normal of openness were presumptively applicable, cogent reasons could be found for departure from the norm in the particular case.[449]

In rejecting the role of judicial function in defining the nature of a court, Jaconelli emphasised the role of established practice. However, Baker considered 'the concept of a court is complex and changeable' and more 'the outcome of history, not the reflection of some constant truth which transcends history'.[450] The 'court' may refer to jurisdiction, to the court as an institution or to the court as a corporate body.[451] The concept of a court evolved in the UK from being 'regarded as not merely a place, or an isolated meeting, but a continuous body with a collective mind of its own'.[452]

> Since the court remembered the past and governed the future through its record, which was incontrovertible, it was possible for business to be transacted outside the physical confines of the court and outside the hours of sitting, and yet to be recorded as having been done in court, and therefore in law.[453]

The recent development of virtual courts with transactions outside 'the physical confines of the court' and court hours is not so revolutionary when considered within the confines of this legal fiction referred to by Baker. However, this is not to undermine the principle of open courts as explained by Coke.

[448] See details of eCourtroom times and procedures in Chapter Five of this thesis.
[449] Jaconelli, above n 406, 68.
[450] John Hamilton Baker, *The Legal Profession and the Common Law: Historical Essays* (Hambledon Press, 1986), 153-169.
[451] Ibid 156-169.
[452] Ibid 161.
[453] Ibid 162.

> all caufes ought to be heard, ordered, and determined before the judges of the kings courts openly in the kings courts, whither all perfons may refort; and in no chambers or other private places: for the judges are not judges of chambers but of courts …[454]

More recently in *Assistant Commissioner Condon v Pompano Pty Ltd*[455] French CJ set out some important characteristics of courts. These included, 'the reality and appearance of decisional independence and impartiality'; 'the application of procedural fairness'; 'adherence as a general rule to the open court principle'; and 'the provision of reasons for the courts' decision'. These his Honour found were not absolutes and the open court principle was one that could be qualified by 'public interest considerations such as the protection of sensitive information and the identities of vulnerable witnesses'.[456]

Nettheim identified instances where there can be a conflict between the principle of open justice and due administration of justice: first, in the control of public attendance in court; second, the sensitivity of trial participants where people may find it difficult to testify knowing that there is 'free reporting' in the court; and third, the publicity which may be seen as likely to prejudice the fairness of a trial. [457] These issues have required further examination in the digital world.

Access and openness in court proceedings have become more negotiable online. Paradoxically as technologies provide more instant access and transparency they also pose a more immediate threat to the administration of justice and have demanded a renegotiation of open justice.

2.4.3 Access to information

An understanding of what open access to information means has changed with online delivery of data. Information can be accessed quickly from a computer or mobile device, no longer requiring tedious searches through hard copy court records. This process has been referred to as 'practical obscurity'[458] or the 'inaccessibility of individual pieces of information or

[454] Edward Coke, *The Second Part of the Institutes of the Laws of England: Containing the Exposition of Many Ancient And Other Statues* (Printed for E and R Brooke, Bell-Yard, near Temple Bar, 1797) 130.

[455] *Assistant Commissioner Condon v Pompano Pty Ltd* (2013) 252 CLR 38.

[456] *Assistant Commissioner Condon v Pompano Pty Ltd* (2013) 252 CLR 38, 72.

[457] Garth Nettheim, 'Open Justice Versus Justice' (1985) *The Adelaide Law Review* 587.

[458] The term 'practical obscurity' was discussed by the U.S. Supreme Court in *U.S. Department. of Justice v Reporters Committee* 489 U.S. 749 (1989) in relation to the privacy interest in rap sheets held by government agencies, despite much of the information being a matter of public record. Rap sheets are prepared by the Federal Bureau of Investigation in the United States and consist of accumulated information on over 24 million people. They contain information such as, date of births, physical characteristics, history of arrests, charges, convictions and

documents created, filed and stored using traditional paper methods relative to the accessibility of information contained in or documents referred to in a computerized compilation'.[459] The disclosure of information which would be hard to find without 'compilation' was found by the Supreme Court of the US to raise distinct privacy issues in *US Department of Justice v Reporters Committee*[460]. Justice Stevens found that '[p]lainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information'.

The fact that personal data has been disclosed in a different form or by a different method does not lessen the concern for privacy. In *Department of Air Force v Rose*[461], despite the Air Force Academy Honour and Ethics Code case summaries having been publicly posted on 40 squadron bulletin boards, the issue of practical obscurity was considered. It was held that if the deletion of personal reference and identifying information was not sufficient to protect the privacy of the individuals concerning the summaries, they should not be released. Although considering the personal information previously released and that 'no one can guarantee that all those who are "in the know" will hold their tongues, particularly years later when time may have eroded the fabric of cadet loyalty', in the past it would have been sufficient to provide privacy protection but not in the era of compilations and computer accumulation and storage.

A significant source of obscurity has been found in the 'modern tendency to place much greater reliance upon documentary evidence and written submissions rather than oral' submissions.[462] Legal arguments are often presented in written form with submission

incarcerations. They are normally preserved until the person turns 80 years of age. It was considered that rap sheets contain information that would have been forgotten except for the computer aggregation. It was considered that due to the volume of rap sheets 'they are sometimes incorrect or incomplete and sometimes contain information about other persons with similar names'. In this case CBS news correspondent and the Reporters Committee for Freedom of the Press requested information about the criminal records of four members of the Medico family because the family's company, Medico Industries was identified by the Pennsylvania Crime Commission as dominated by organized crime figures and had obtained a number of defence contracts due to an improper arrangement with a corrupt Congressman. The Supreme Court considered the application of Exemption 7(C) which required them to balance the privacy in maintaining the "practical obscurity" of the information against the public interest in their release.

[459] Judges Technology Advisory Committee (Discussion paper, Canadian Judicial Council, *Open Courts, Electronic Access to Court Records, and Privacy*, May 2003) <http://www.cjc-ccm.gc.ca> 29.

[460] *Department of Air Force v Rose* 489 U.S. 749 (1989) where it was held that the privacy interest in maintaining the practical obscurity of rap-sheet information would always be high and therefore the disclosure of the contents of the FBI rap sheet to a third party could be reasonably expect to constitute an unwarranted invasion of person privacy within Exemption 7(C) of the *Freedom of Information Act*.

[461] *Department of Air Force v Rose* 425 U.S. 352 (1976).

[462] Martin, above n 422, 10.

provided to the court before the hearing.[463] Willheim questioned the transparency and openness of courts and argued that as 'issue of fact are determined by reference to evidence that is not publicly available' it has become difficult for members of the public to follow the oral argument which is often an elaboration of written material unavailable to them.[464] He considered that courts should give 'reasonable access to all material admitted in evidence and to written submissions'[465] despite the demands of procedures adopted to improve the efficient administration of justice.[466] Obscurity in a physical courtroom can also result from simple problems such as 'poor sightlines and audibility' in the physical courtroom[467] or the use of technical language.

This practical obscurity of legal information disclosed in the courtroom has been removed by technical developments which make all information potentially available for disclosure. This open access in itself has created complications. Following the extensive technological access to online court records by PACER[468] by the federal courts in the US, considerable problems relating to the protection of privacy arose. New court rules were introduced to 'intentional inconvenience' and restrict access, which was a 'modern creation of practical obscurity',[469] particularly in actions for social security benefits and in immigration cases relating to removal, benefits or detention. Access was made available only at terminals at the courthouse and remote access denied.

Eltis distinguished 'accessibility' in the pre-electronic era to the present where there is 'an audience of incalculable numbers with indiscriminate access' allowing access to personal,

[463] Federal Court of Australia Practice Note APP 2 deals with the content of appeal books and preparation for hearing: 5.1 of APP 2 provides that "[e]ach party must prepare an outline of that party's submissions" and 5.9 provides, "It is expected that oral arguments will follow the outline of submissions. New issues, not included in the outline, may not be advanced on the hearing except with the leave of the Court".

[464] Willheim, above n 377, 197.

[465] Ibid 204.

[466] Ibid 203.

[467] Martin, above n 422, 9.

[468] The Public Access to Court Electronic Records (PACER) si an electronic public access service that allows users to obtain case and docket information online from federal appellate, district, and bankruptcy courts in the US. It has millions of case files documents. The PACER website provides access to the Case Management/Electronic Case Files and allows courts to accept filings and provides access to filed documents online. <https://www.pacer.gov>.

[469] Center for Legal & Court Technology, 'Public Access to Court Electronic Records in the Age of eFiling' (Paper presented at the 9th conference on Privacy and Public Access to Court Records, William & Mary Law School, Williamsburg, 14-15 October 2013) <http://www.legaltechcenter.net/education/conferences/9th-conference-on-privacy-public-access-to-court-records/>.

sensitive information 'in an unprecedented fashion'.[470] This new accessibility has been shown to lead to distorted profiles particularly through the use of search engines such as Google. The inaccurate and often misleading data can be obtained by aggregation of often unrelated information. The decision of *Helow v Scotland (AG)*[471] was used to illustrate how information discovered by the use of a search engine revealed misleading data. In this case the judge was 'googled' and it was discovered that she was a member of the International Association of Jewish Lawyers and Jurists. It was alleged by the appellant, a Palestinian seeking a refugee asylum in the UK, that membership of such an organisation alone demonstrated apparent bias.[472] The case was described as a 'warning to judges regarding the ready dissemination of personal and unrelated information over the internet, its availability to litigants, and the potential for resulting frivolous claims or manipulation'.[473] It also raised the recurring question of the relevance of personal data about judges. The United Sates Department of Justice[474] has warned of a 'web-*industry*' dedicated to collection information from court records with the object of 'intimidation and retaliation'. Snyder concluded that the 'remote electronic availability and dissemination of judicial documents may come at a considerable cost' which includes the intimidation of witnesses, retaliation and harassment.[475]

Documents are more easily accessed via websites and remain permanently available, unlimited by court registry times. This has provided additional publicity for the names of the personnel and details of the trial, challenging the courts' control over its own data. Bellis has observed that '[t]he evolution of contemporary trial and case management practices also has important implication for the full and effective observation of the open principle through access to court records'. Without such access 'it is extremely difficult – even for an observer in the courtroom – to understand the nature of the case, the scope and significance of the evidence presented or the legal arguments advanced'.[476] She found that in Australia there is no common law

[470] Eltis, above n 413, 289.
[471] *Helow v Scotland (AG)* [2007] CSIH 5 at [16]; [2008] UKHL 62 2 All ER 1031.
[472] *Helow v Scotland (AG)* [2007] CSIH 5 at [16]; [2008] UKHL 62 2 All ER 1031 – it was held that a fair-minded and informed observer, having considered the relevant facts, would not conclude that there was a real possibility that the judge had been biased by reason of her membership of the association.
[473] Eltis, above n 413, 299.
[474] Michael A Battle, Director, Executive Office for U.S. Attorneys, U.S. Department of Justice, letter to James C Duff, Secretary, Judicial Conference of the U.S. (6 December 2006) <http://www.floridasupremecourt.org/pub_info/summaries/briefs/06/06-2136/Filed_01_31_2007_ProsecutorsSupplementalCommentsAppendix.pdf>.
[475] David L Snyder, 'Nonparty Remote Electronic Access to Plea Agreements in the Second Circuit' (2009) 35 *Fordham Urbane Law Journal* 1263, 1265.
[476] Bellis, above n 371, 200.

presumption of accessibility to court records and the legislation and rules that govern public access to court records vary from those that are largely unrestricted to very limited access.[477]

However, in the US, the Supreme Court has recognised a common law right to inspect and copy public records.[478] Online access to electronic court records[479] are available for all courts at the federal level in the US with some restrictions, due mainly to privacy concerns. Certain information must be redacted from documents before filing, including such information as financial account numbers, dates of birth, social security and taxpayer identification numbers. The Judicial Conference Privacy Policy also established a category of documents which should not be included in public case files or made available. These include documents such as juvenile records; sealed documents; unexecuted summonses or documents containing identifying information about jurors or potential jurors.[480] There are also a variety of court rules, designed by reference to the Judicial Conference Privacy Policy which prescribed requirements for sealing documents. In addition federal court website contain privacy notices which 'caution about the implications of filing other kinds of potentially sensitive information' such as employment history, medical records and trade secret information.[481]

Banisar considered that the UK 'should adopt a similar system of proactive disclosure' as in the US where the PACER system which allows most electronically documents to be accessed by anyone for a small fee.[482] This is because of the legal and practical limits to open justice. These include the 'more document-focused case system', fewer reporters in courts, limitations on the availability of transcripts, limits to the video and audio recording of cases and limited application of the *Freedom of Information Act 2000* (UK).

Some of the problems relating to increased openness of court processes have been identified in an examination of public records on the internet in the US.[483] These include: the possible

[477] Ibid 201-207.
[478] Ibid 212.
[479] *E-Government Act of 2002*, 44 USC § 101 (2002).
[480] Bellis, above n 371, 213.
[481] Ibid 214.
[482] David Banisar, 'Catching Up with the Transparency Revolution' (Paper presented at the Justice Wide Open conference, City University, London, 29 February 2012 <https://openacess.city.ac.uk/1926/1/JWO.pdf >.
[483] Beth Givens, 'Public Records on the Internet: The Privacy Dilemma' (Paper presented at the 12th Annual Conference on Computers, freedom and privacy, San Francisco, 16 – 19 April 2002) <https://www.theguardian.com/commentisfree/libertycentral/2012/apr/03/guardian-court-victory-transparency>.

chilling effect of increased publicity which would discourage participation in public life; the possibility of identity theft using freely available information; the safety risks from violence and stalking when it is easier to locate people; the secondary use of public data, especially following aggregation of information from different and disparate sources; and the permanency of information which can lead to minor crimes in the past preventing future employment in a 'dossier society'. The solutions presented were: to limit the data posted online; introduce automatic redaction systems; 'robust rules of court'; analysis of the public policy objectives of online records; restricting access, particularly to sensitive personal information; anonymising data; regulating private industry to limit background checks and the purchasing of private information, and the implementation of a careful and incremental approach to posting public records online.

Bellis cautioned that while electronic access to court records can enhance access to justice, promote public understanding of the judicial process, improve accuracy and timeliness of media reporting, there is an increased risk to privacy and security which has been recognised in the US, Canada and in Australia.[484] She noted that in Australia the potential risks were not as broad as in the US and Canada as all court records as not presumptively accessible. Bellis recommended that a public education program should be implemented to provide information about the protection of sensitive information. Also Bellis recommended that a court records management system should developed that allows different levels of permission for access and a 'coherent classification for all court records when they are filed and deployed'.[485] An enhanced right of electronic access for the media was advocated because professional journalists were seen as being trained about the legal limitations on the use of court records, the potential harm and consequent penalties. Bellis also considered that 'public access for commercial uses unrelated to the judicial proceedings is inconsistent' with privacy principles and therefore use of personal information should be limited to the specific use for which it was provided.[486] She recommended a national collaboration of court officials and government policy-makers to develop and implement consistent, transparent regime of access to court records to ensure the benefits of technology were retained and social interests and values protected.[487]

[484] Bellis, above n 371, 229-230.
[485] Ibid 230.
[486] Ibid 231.
[487] Ibid.

Bepko[488] questioned whether internet access should be treated differently. A tension between what was perceived to be private and what ought to be private was identified as a contentious issue, particularly whether information which is freely available at local courthouses should also be available on the internet. Bepko concluded that 'the presumption in favor of public access to court documents should not shift depending on the medium'.[489] While it was conceded that the internet is 'decidedly different from the courthouse' in the time it takes to circulate, view and copy documents and impossible to conceal, courts can seal and redact sensitive information at litigant's requests.[490] The dangers associated with compiled information, the chilling effect of personal information available through court filings and the deliberate misuse of personal data were dismissed as reasons for not providing internet access. It was argued that the information available for compilation is a part of the public court record and internet access would only make access faster. Bepko did not see any danger in the availability of personal information which can be protected by redaction and appropriate advice. As well, this personal information was thought to be a possible 'empowering tool for victims' by allowing them to conduct their own investigations.[491]

The open access to court documents promised by technological change has not been delivered without limitations. The access has paradoxically been restricted by concerns for the security and privacy of personal data and the introduction of new procedures such as the increased provision of electronic material being used in court proceedings. It has raised the question of what access rights people who are not parties to the case being heard have to this material and how open such access should be.

2.4.4 Publicity of proceedings

Reporting of the proceedings has also been viewed as an essential element of openness for the courts.[492] Technological developments have dramatically altered communication between the courts and the public. The press no longer have the special role in the communication chain. This has been transformed by OSNs with some courts reporting directly via Twitter to the public and reporters themselves, when allowed by the courts to send Tweets from court.

[488] Arminda Bradford Bepko, 'Public Availability or Practical Obscurity: The Debate over Public Access to Court Records on the Internet' (2005) 49 *New York Law School Law Review* 967.
[489] Ibid 968.
[490] Ibid 989.
[491] Ibid 987.
[492] See comments by Lord Diplock in *Attorney-General v Leveller Magazine* [1979] AC 450 with regard to publication to a wider public.

Interactive applications have enabled anyone with a mobile phone or computer to report, blog, tweet and comment on legal decisions.

The media, from the 19th century, had become the 'purveyors of information about the courts' with 'the principle of open justice as embracing the right of the public to receive media reports about the workings of the courts'.[493] For courts to physically open their doors, has been recognised, as insufficient in modern times because 'the reality is that most people do not avail themselves of their right to attend judicial proceedings, nor do they acquire information by word of mouth from those who have'.[494]

In 2014 in *Marsh v Baxter*[495] Justice Kenneth Martin confronted the issue of the 'capacity of modern courts to facilitate interested members of the community reliably informing themselves about a trial',[496] if they cannot attend. His Honour noted the role in the past of the media in informing the public but considered in the electronic era people expect 'more direct immediate involvement' and access to tendered documents, transcript, written submissions and witness statements. In *Marsh v Baxter* the court assisted access to information about the proceedings by publishing a progressive release of the daily transcript on the court website, providing opening and closing written submissions, expert reports and various witness statements to advance 'public confidence in the integrity and independence of the judicial system'.[497] His Honour referred to procedural changes in 2014 in Western Australian courts to allow live tweets from courts and the use of electronic devices, such as smart phones and laptops by the media and legal practitioners.[498] Reference was also made to public access online in *Essendon v ASADA*[499] due to public interest in this matter. The hearing before Justice Middleton in August 2014 was televised.

[493] Sharon Rodrick, 'Open Justice, the Media and Avenues of Access to Documents on the Court Record" (2006) 29 *UNSW Law Journal* 90.
[494] Ibid.
[495] *Marsh v Baxter* (2014) 46 WAR 377; [2014] WASC 187. This was a high profile case of considerable public interest due to the grievance of the Marshes concerning the use of GM canola crops on a neighbouring farm. It was alleged, the seed pods from the canola crop had blown over from Mr Baxter's farm and had damaged their organically grown cereal crops and organic lamb certification. The case was considered of significance to the farming community in Western Australia.
[496] Kenneth Martin, Justice (ed) 'Open Justice in Western Australia' (2014) 88 *Australian Law Journal* 779-781, 779.
[497] Ibid 780.
[498] Ibid.
[499] *Essendon Football Club v Chief Executive Officer of the Australian Sports Anti-Doping Authority* (2014) 227 FCR 1, Middleton J, 19 September 2014. <http://www.fedcourt.gov.au> This case concerned an application challenging the power of the CEO and ASADA to conduct a joint investigation into the Essendon Football Club players and personnel involved in a supplements program implemented by Essendon in 2011 and 2012.

Conflict between the principle of openness and the due administration of justice has been recognised where certain forms of publicity could possibly prejudice a fair trial; when it may be difficult for witnesses to testify in open court or people deterred from institution proceedings; or where it is necessary to control public attendance.[500] The fair and accurate reporting of court proceedings was considered by McHugh JA to be essential to ensuring that the public know what is happing in the courts and prevent 'rumours, misunderstandings, exaggerations and falsehoods which are so often associated with secret decision making'.[501] This reporting is inherent in the modern concept of open justice and 'requires that nothing should be done to discourage the making of fair and accurate reports of what occurs in the court room'.[502] The Court of Appeal (Victoria) considered that '[a] court is "open" when, at the least, members of the public have a right of admission'. From this it may be thought ordinarily to follow that the media, in their various forms, are also entitled to communication 'to the whole public what that public has a right to hear and see'.[503]

Under common law in Australia the principle of open justice can be departed from if it is 'really necessary to secure the proper administration of justice'.[504] Chief Justice French of the High Court of Australia considered that 'necessary' did not mean 'convenient, reasonable or sensible or to serve some notion of public interest'[505] in the context of the statutory provision. His Honour considered:

> there is inherent jurisdiction or implied power in limited circumstances to restrict the publication of proceedings conducted in open court. The exercise of the power must be justified by reference to the necessity of such orders in the interests of the administration of justice.[506]

In addition to the common law, French CJ considered that orders to prevent or restrict publication of parts of proceedings, could be made by parliaments.[507] The term 'necessary' has been held to be a strong word not 'concerned with trivialities'.[508] The rationale of the principle being to subject court proceedings to public and professional scrutiny and maintain

[500] Garth Nettheim, 'Open Justice Versus Justice' (1985) 9 *Adelaide Law Review* 487-518.
[501] *John Fairfax & Police Tribunal of New South Wales* (1986) 5 NSWLR 465, 481.
[502] *John Fairfax & Sons Ltd v Police Tribunal of New South Wales* (1986) 5 NSWLR 465, McHugh JA, 476.
[503] *Re Applications by Chief Commissioner of Police (Vic)* (2004) 9 VR 275 [25].
[504] *John Fairfax & Sons Pty Ltd v Police Tribunal of New South Wales* (1986) 5 NSWLR 465, McHugh JA.
[505] *Hogan v Australian Crime Commission* (2010) 240 CLR 651, 664.
[506] *Hogan v Hinch* (2011) 243 CLR 506, 543.
[507] *Hogan v Hinch* (2011) 243 CLR 506, 534 where reference was made to s 50 *Federal Court of Australia Act 1976* (Cth); the *Crimes Act 1914* (Cth) and numerous State Acts such as *Court Suppression and Non-publication Orders Act 2010* (NSW); *Witness Protection Act 1995* (NSW); *County Court Act 1958* (Vic); *Children's Protection Act 1993* (SA) and the *Supreme Court of Queensland Act 1991* (Qld).
[508] *ACCC v Air New Zealand Limited (No 4)* [2012] FCA 1439, [4] (Perram J).

public confidence in the courts.[509] However, the application of the principle can be limited where the character of the proceedings and the nature of the function conferred upon the court may dictate this.[510] Examples provided by French CJ were: where the proceeding involved a secret technical process such that the whole matter in dispute would be destroy by disclosure; injunctive relief against an anticipated breach of confidence; the protection of a witness, such as a blackmailer's victim, where if not protected other complainants may not give evidence; similarly the name of a police informant may require protection; the 'exceptional and compelling considerations going to national security'; proceedings relating to wards of the State and mentally ill which were historically exceptions or other proceedings not 'in the ordinary course of litigation'.[511]

Justice Rares has noted the importance of publicity and recognised that everyone should have 'a right to publish a fair and accurate report of court proceedings which is of fundamental importance':[512]

> The more paper or electronic material before the court, the less likely it is that the observer will obtain adequate information as to the judicial process he or she observes, unless that written or electronic material is publicly available.[513]

His Honour noted the issue in the digital era with the production of electronic material which will make it more difficult for an observer of the court process to obtain the necessary information to understand court proceedings. The boundary between what can be published to provide open justice and what will infringe on the administration of justice needs to be redefined in the digital era.

2.5 The cost of open access in the digital era

The cost of access to justice can be assessed in tangible and intangible terms. Tangible costs of access to justice have been the subject of extensive analysis and research, such as the work of the Productivity Commission discussed in the previous chapter, in the objective of successive governments to find budget savings. Assessing intangible costs is more challenging, however it is the intangible costs, in particular the costs of disclosure of personal

[509] *Hogan v Hinch* (2011) 243 CLR 506, 530, French CJ.
[510] *Hogan v Hinch* (2011) 243 CLR 506, 531, French CJ.
[511] *Hogan v Hinch* (2011) 243 CLR 506, 532.
[512] Justice Steven Rares, 'How the implied Constitutional Freedom of Communication on Government and Political Matter may require the Development of the Development of the Principles of Open Justice' (Paper presented at the Judicial Conference of Australia Colloquium, Sydney, 7 October 2007) 4.
[513] Ibid 27.

information, that is subject of analysis in this thesis and the way in which digital access to justice can be achieved without compromising privacy.

Friedman questioned the desirability of expanding access when the cost for increasing access was the loss of 'the right which we vaguely call "privacy", the zone of immunity that surrounds our life and protects our idiosyncrasies'[514] where such '[e]asy access may impair the value which we place on being left alone'. He found the modern American 'adversarial legalism' to be 'pathologically open' providing 'so much access that plans, projects, and rules die a slow and lingering death, smothered by lawsuits and murdered through litigation'[515]. Friedman concluded that access to justice is complex, a matter of procedure, 'deeply substantive and normative' with the solution to be found in 'how the problem is defined and what policy goals one wishes to reach'.[516]

The issue of privacy in applications for confidentiality has always been an important consideration and not one just associated with digital access, as Lord Keith noted in 1983 in *Harman v Home Office*:

> Discovery constitutes a very serious invasion of the privacy and confidentiality of a litigant's affairs. It forms part of English legal procedure because the public interest in securing that justice is done between parties is considered to outweigh the private and public interest in the maintenance of confidentiality. But the process should not be allowed to place upon the litigant any harsher or more oppressive burden than is strictly required for the purpose of securing that justice is done. In so far as that must necessarily involve a certain degree of publicity being given to private documents, the result has to be accepted a part of the price of achieving justice. But the fact that a certain inevitable degree of publicity has been brought about does not, in my opinion, warrant the conclusion that the door should therefore be opened to widespread dissemination of the material by the other party or his legal advisers, for any ulterior purpose whatsoever, whether altruistic or aimed at financial gain. The degree of publicity resulting from a document being read out in open court is not necessarily very great. There may be nobody present apart from the parties and their legal advisers. The argument for the appellant, however, goes the length that because the public are notionally present, and anyone might have come in and noted down the contents of any discovered document which is read out, the implied obligation against improper use comes to an end.[517]

The appellants in this case argued that the public were 'notionally present' and could write down the details when the documents were read in court. This submission was not accepted

[514] Lawrence M Friedman, 'Access to Justice: Social and Historical Context' in Volume 1 of *Access to Justice* series by Mauro Cappelletti and Bryant Garth (eds) 35.
[515] Lawrence M Friedman, 'Access to Justice: Some Historical Comments' (2009) 37 *Fordham Urban Law Journal* 3, 6.
[516] Ibid 15.
[517] *Harman v Home Office* [1983] 1 AC 280 at 308.

by the judge who referred to the implied obligation not to make improper use of discovered documents which is independent of confidentiality obligations and provides protection in the interests of the proper administration of justice.[518]

While the test of 'necessity' has developed as the test for Australian courts in determining whether non-publication orders are to be issued, the question is whether this test needs further clarification in an open digital environment. The access to information now possible online which is available instantly and to 'a vast audience that transcends jurisdictional borders'[519] has the potential to prejudice the administration of justice. Courts are able to use statutory exceptions to the principle of open justice, although there is no inherent power to close a court. These provisions protect privacy and prejudice to the administration of justice.

The involvement of high profile families, such as the Rinehart family,[520] in litigation has led to rigorous attempts to suppress information, particularly with the widespread dissemination and permanency made possible on the internet. The power to make an interim suppression order and whether it was necessary to prevent prejudice to the administration of justice was considered in *Rinehart v Welker* (*Rinehart* litigation) in 2011 and in a number of related cases.[521] The Court of Appeal in 2011 reviewed a decision of Tobais AJA to impose a suppression order which prohibited publication of the majority of documents filed and others made in the proceedings.[522] The proceedings had been commenced by ex parte application. The trustee sought a stay of the proceedings and a suppression order on the basis that the proceedings were an abuse of process. An interim suppression order had been granted pending the determination of an application for leave to appeal where Tobian AJA considered the administration of justice would be prejudiced if the order was not made[523].

[518] *Harman v Home Office* [1983] 1 AC 280 at 308.

[519] Brian Fitzgerald and Cheryl Foong, 'Suppression Orders after *Fairfax v Ibrahim*: Implications for Internet Communications' (2013) 37 *Australian Bar Review* 1.

[520] Extensive litigation in the Supreme Court of NSW and the Federal Court, concerning applications for suppression orders and access to documents involving the Rinehart family was discussed in detail by Miiko Kumar, 'Keeping Mum: Suppression and Stays in the Rinehart Family Dispute' (2012) 10 *Macquarie Law Journal* 49.

[521] The *Rinehart* matters have a long and complex litigation history of numerous applications for a stay of proceedings and suppression orders from 2011 to 2014 in the New South Wales Supreme Court and the Federal Court; *Rinehart v Welker* [2011] NSWCA 345; *Welker v Rinehart* [2011] NSWSC 1094; *Rinehart v Welker* [2012] NSWCA 1; *Bianca Hope Rinehart v Georgina Hope Rinehart* [2014] FCA 1241: *Rinehart v Rinehart (No 2)* [2015] FCA 339.

[522] *Rinehart v Welker* [2011] NSWCA 403 (7 December 2011) Young JA [57].

[523] *Rinehart v Welker* [2011] NSWCA 345 (31 October 2011) [43].

The Court of Appeal considered s 8 of the *Court Suppression and Non-Publication Orders Act 2010* (NSW) and the operative condition that it be 'necessary' to make such an order.[524] Chief Justice Bathurst and McColl JA referred to the observations in *Hogan v Australian Crime Commission*[525] which required the court to exercise jurisdiction in open court. The key principles were;: first the order must be 'necessary'; second, the principle of open justice is 'one of the most fundamental aspects of the system of justice in Australia'; third, the court must take into account a 'primary objective of the administration of justice is to safeguard the public interest in open justice' fourth, 'the necessity principle encapsulates as its final and paramount consideration the need to do justice. Publication is a means to that end and can only be avoided where necessity compels departure from the open justice principle: fifth, 'the right of media to report on court proceedings is a corollary of the right of access to the court by all members of the public'; sixth, if there is embarrassment and damage to the parties' reputation inherent in the litigation, that is the price of open justice; seventh there are exceptions to the principles of open justice which may be made if openness would 'destroy the attainment of justice' and finally 'in a free society public access to the conduct of courts and the results of deliberations in the courts is a human right'.

Justice Jacobson in *Rinehart v Rinehart*[526] also referred to the long line of authorities which discuss the key principles[527] commented on the role of s 37AE of the *Federal Court of Australia Act* (Cth) which reinforces the necessity principle.

Protecting personal data from online disclosure has become increasing difficult[528], particularly for jury trials. Burd and Horan[529] recognized a growing tension between the principles of open justice and the right to a fair trial particularly as 'anyone can be a publisher on the internet'. The change in communication and dissemination of information to a world where, '[n]ewspapers are read online, televised broadcasts are stored and watched on YouTube, radio

[524] *Rinehart v Welker* [2011] NSW CA 403 Bathurst CJ and McColl JA at [27].

[525] *Hogan v Australian Crime Commission* (2010) 240 CLR 651, 664.

[526] *Rinehart v Rinehart* [2014] FCA 1241.

[527] *Hogan v Australian Crime Commission* (2010) 240 CLR 651; *Hogan v Hinch* (2011) 243 CLR 506; *John Fairfax and Sons Ltd v Police Tribunal of New South Wales* (1986) 5 NSWLR 465 and *John Fairfax Publication Pty Ltd v District Court of NSW* (2004) 61 NSWLR 344.

[528] Isaac Frawley Buckley, 'In defence of "take-down" orders: Analysing the alleged futility of the court-ordered removal of archived online prejudicial publicity' (2014) 23 *Journal of Judicial Administration* 203 – an analogy has been drawn between the orders of King Canute (early king of England, Denmark, Norway and parts of Sweden – 985-1035 AD) to the sea to stop the rising tide and futile take-down orders because removing articles from one website does not mean that they will be unavailable on other web sites or in the public domain.

[529] Roxanne Burd and Jacqueline Horan, 'Protecting the right to a fair trial in the 21st century – has trial by jury been caught in the world wide web?' (2012) 36 *Criminal Law Journal* 103, 105.

segments are available via podcasts, Facebookers, bloggers and tweeters can share ideas, opinions and images with the world at large'. Because Facebook information, blogs and YouTube videos can be downloaded by jurors, even on their mobile phones, Burd and Horan concluded that the traditional approach of preventing prejudicial publicity is failing due in no small part to the new technological developments and will likely further challenge the right to a fair trial. It was considered that 'sub judice contempt and suppression orders have a role to play in criminal procedure, they are not foolproof mechanisms for ensuring a fair trial for infamous defendants because anyone can publish on the internet'. [530] Possibly solutions suggested were trial by judge alone or a trial by a mixed jury[531] consisting of lay assessors and professional arbitrators.

The impact of the new regulatory environment and the effectiveness of court orders made to provide a fair trial to the accused were clearly demonstrated in *News Digital Media Pty Ltd v Mokbel*[532] where it was found that 'the mischief to which the internet order was directed was the danger caused by the maintenance of the website publication, rather than their being posted on the websites'.[533] The necessity and utility of take-down orders were considered in *News Digital Media Pty Ltd v Mokbel.*[534] While the trial judge agreed with the submission that the order should be made because the information on the websites of media organisations have considerable credibility and therefore impact on the mind of jurors, on appeal it was held that the order was not necessary for the protection of the court process. The removal of the material did not prevent a determined searcher from accessing it from a cached website.[535]

Chief Justice Warren and Byrne AJA held that it was 'the interposition of the internet which causes the particular difficulty in this case'. Four different characteristics of the internet were identified: the first, 'it is permanent' and may become 'a different publication' by being recorded in sound and pictures; second, the publication lacks a specific location and therefore

[530] Ibid 122.

[531] Ibid 119-120: The earliest idea of a mixed jury was traced to England in the 12th century while the modern one was seen as having its roots in civil law countries such as Germany and France. The advantages were considered to be the reduced likelihood that jurors would share their own research and the additional guidance professional arbitrators could provide to the lay jurors.

[532] *News Digital Media Pty Ltd v Mokbel* (2010) 30 VR 248.

[533] *News Digital Media Pty Ltd v Mokbel* (2010) 30 VR 248, 265.

[534] *News Digital Media Pty Ltd v Mokbel* (2010) 211 A Crim R 292, 312.

[535] Buckley, above n 514, 211: see also Jacob Rowbottom, 'Holding Back the Tide: Privacy Injunctions and The Digital Media' (2017) 133 *Law Quarterly Review* 177-183. In this article Rowbottom distinguished *Mosley v News Group Newspapers* [2008] EWHC 687 as an extreme case, one in which an interim injunction was not granted due to widespread internet publications. He discussed the dilemma faced by courts when information circulating in digital media threatens to compromise the effectiveness of privacy injunctions, placing the courts in "no win" situations.

may be accessed by potential jurors locally, interstate or overseas, so limiting the effectiveness of 'court processes of injunction or the threat of prosecution for contempt';[536] third, the information is available by searching the internet where publications can be found by searching a string of words and are 'very readily and virtually instantaneously retrieved, downloaded and opened';[537] and fourth, 'a feature of the publication of an article on an internet website is that it is available to be copied and posted on other websites outside Victoria'.[538]

Bosnall and Bagnall considered *Mokbel* an important decision in distinguishing general suppression orders from 'proceedings suppression orders'. The two types of suppression orders were held to raise very different policy and jurisdictional issues. Orders to retrain the publication of the three proceedings concerning Mr Mokbel were seen as raising the issue of administering justice in public (open justice) and the general suppression order concerning the publication of specific matters concerning Mr Mokbel as fulfilling the requirement that the accused is entitled to trial by an impartial tribunal ('freedom of speech or the public's "right to know"'). Whatever the policy and jurisdictional issues distinguishing these suppression orders, whether they are granted or not does concern the issue of access to information. The reference to 'suppression' was also considered inapt with the more neutral term 'non-publication orders' or 'postponement orders' considered more appropriate because the purpose and effect of the order is postponement of publication rather than suppression.

Suppression or non-publication orders have been important in 'shaping the relationship between law and the media'[539]. It has been alleged that '[s]uppression orders are more powerful than ever, but they're also more ineffectual'.[540] Research into the rate of suppression orders by Victorian courts between 2008 and 2012 revealed that the 'overall numbers were high (and appear to be increasing) and there are significant and widespread problems with the duration, scope and clarity of orders'.[541]

[536] *News Digital Media Pty Ltd v Mokbel* (2010) 30 VR 248, 268.
[537] *News Digital Media Pty Ltd v Mokbel* (2010) 30 VA 248, 269.
[538] *News Digital Media Pty Ltd v Mokbel* (2010) 30 VA 248, 270.
[539] Andrew T Kenyon, 'Not Seeing Justice done: Suppression Orders in Australian Law and Practice' (2006) 27 *Adelaide Law Review* 279, 282.
[540] Myriam Robin, 'You can't shut down the internet': the futility of suppression orders' (28 November 2014) *Daily Telegraph*.
[541] Jason Bosland and Ashleigh Bagnall, 'An Empirical Analysis of Suppression Orders in the Victorian Courts: 2008-12' (2013) 35 *Sydney Law Review* 671, 702. This article referred to a 2008 study chaired by Prue Innes ('*Innes Study*') which reported between 2006 and 30 June 2008, 649 suppression orders had been issued by the Victorian courts but only 54 order made in New South Wales.

Reference was also made to s 6 of the *Court Suppression and Non-Publication Orders Act* which provided that orders should only be made in exceptional circumstances.[542] This section reinforces what the court should take into account where considering whether to make a suppression order which is that 'a primary objective of the administration of justice is to safeguard the public interest in open justice'.[543] The right of the media to report on court proceedings was discussed. It was held that the media had standing and were entitled to report as 'a corollary of the right of access to the court by members of the public'.[544] The Court of Appeal ordered that the orders of Tobias AJA were to be discharged because it was not considered necessary to prevent prejudice to the administration of justice and to make such a suppression order would 'undermine, rather than ensure, public confidence in the administration of justice'.[545]

The futility of using 'take-down' orders to remove archived online publicity which could prejudice a fair trial were examined in the context of the changed online media landscape. Buckley's[546] article focussed on the ability of courts to make orders preventing 'contemptuous material from interfering with the administration of criminal justice in jury trials'. It was found that most news articles are now archived on news organisations' websites and remain accessible to the public without the need to search back copies of newspapers in libraries in hard copy or on microfiche. These articles may 'no longer be appropriate, acceptable or permitted by laws governing publication (such as defamation or sub judice contempt)', yet they may have the potential to impact on the administration of justice when googled by jurors. These archived articles have been held to be 'a "continuing act"' for the purposes of contempt on each day that it remains accessible'.[547]

Take-down orders target 'historical publications and pre-trial media coverage' which is not connected to proceedings, other than by its capacity to impact on current and future proceedings and the publications could not be the subject of suppression orders.[548] In *Fairfax Digital Australia & New Zealand Pty Ltd v Ibrahim*[549] Basten JA found that a take-down order will

[542] *Rinehart v Welker* [2011] NSWCA 403 (7 December 2011) [27].
[543] *Rinehart v Welker* [2011] NSWCA 403 (7 December 2011) [32]-[33].
[544] *John Fairfax Publications Pty Ltd v District Court (NSW)* (2004) 61 NSWLR 324, 344.
[545] *Rinehart v Welker* [2011] NSW CA 403 (7 December 2011) [55].
[546] Buckley, above n 528, 203.
[547] Ibid 205.
[548] Ibid 209.
[549] Ibid 232.

'not necessarily be futile because material is available otherwise in cached form'.[550] If it is considered futile it will fail the necessity test. Consideration must be made to whether a jury would be likely to abide by directions and not consult such material.

Legislation to 'strengthen and promote open justice in Victoria's courts' was introduced by the Victorian Attorney-General, Robert Clark.[551] He stated that:

> Open justice demonstrates publicly that laws are being applied and enforced fairly and effectively. Unless there is good reason to the contrary, the community is entitled to know what is being said in court where there are allegations that the conduct of an individual or organisation is in breach of the law.[552]

The objective was to set clear rules and guidelines for the making of any orders to suppress publication of matters that might prejudice a fair trial. Orders restricting the reporting of court proceedings can only be made to protect the safety of any person; to prevent prejudice to the proper administration of justice or prejudice to national or international security; to avoid undue distress or embarrassment to a party or witness in criminal proceedings involving a sexual offence or family violence or where there is a child who is a witness in a criminal proceeding. There must be a strong and valid reason for the making of a suppression order, they must be no more than necessary; there must be a restriction on duration and the court must be satisfied on the basis of 'sufficient credible information that the grounds for making a suppression order are established'. Despite the best intentions of these legislative changes, it has been alleged that 'Victoria has become the suppression capital of Australia, if not the world'.[553]

Non-publication and suppression orders may protect private data in the interests of the administration of justice, however, open justice and open court remain an essential consideration. Cannon warned of the dangers of 'unfettered electronic access to court data bases' and advocated the adoption of policies to restrict access and prevent misuse of information. He suggested such measures as storing suppressed information separately, providing access policies to all litigants and obtaining appropriate undertakings from people

[550] Ibid.
[551] Media Release: 'New law to strengthen open justice' (Wednesday 26 June 2013) The Hon Robert Clark MP <http://www.premier.vic.gov.au>.
[552] Ibid.
[553] Rebecca Ritters, 'Mornings with Del Irani' (26 June 2013) <http://blogs.abc.net.au/victoria/2013/06/is-victoria-the-suppression-capital-of-the-world-the-anti-doping-authority-to-get-new-powers-racing-.html?site=milduraswanhill&program=melbourne_mornings>.

searching data bases with disclaimers accompanying information made available.[554] Indiscriminate posting of court records online could exponentially worsen that problem[555] of witness-litigant bullying as well as have a chilling effect on access to justice.

The Lord Chief Justice of England and Wales, Lord Judge, on 14 December 2011 issued guidance on live text-based communications from court to support open justice and stated:

> A fundamental aspect of the proper administration of justice is open justice. Fair, accurate and, where possible, immediate reporting of court proceedings forms part of that principle. [556]

While the judge retains full discretion to prohibit live, text based communications, the overriding responsibility Lord Judge considered was to ensure that there was not 'any improper interference' with court proceedings. Under the guidelines, representatives of the media or a legal commentator are able to use text-based devices for communication from court. This includes using mobile email, social media, including Twitter, and internet enabled laptops in open court. Prohibition on the taking of photographs and use of sound recording equipment without leave remains. However, a member of the public must make an application, either formally or informally to use live text-based communications during court proceedings.

2.6 Conclusion

The more recent technological changes ironically offer openness and access to justice while, at the same time, question the extent openness should be regulated in a complex regulatory environment. In this environment the facilitation of unregulated disclosure, the aggregation and permanency of huge volumes of private data uploaded online and its commodification have increased the challenges for legal protection.

Web 2.0 applications have provided some element of urgency to the issue of competing human rights, such as the conflict between privacy and freedom of speech by facilitating access to personal data online and so raised the need for the development of an efficient regulatory framework. As Chief Justice, Beverly McLachlin has stated, 'open justice … comes

[554] Andrew Cannon, 'Policies to Control Electronic Access to Court Databases' (2001) *Journal of Judicial Administration* 100, 106.
[555] Eltis, above n 399, 301.
[556] 'Practice Guidance: The use of live text-based forms of communication (including *Twitter*) from Court for the purposes of fair and accurate reporting.' (14 December 2011) <http://www.judiciary.gov.uk>.

at a cost. It exists in tension with two other things that we value – privacy and security'.[557] This is a cost which is exacerbated in the online digital era where online social networks, such as Facebook and Twitter, provide a new dimension in social interaction and communication, they have created challenges for the courts by offering direct communication but question how they can be regulated in their negotiable and, at times, anarchical space.

The changes have also challenged the court's control over its own processes. Some indication of the changes has been seen in the increase in applications to suppress information, a reaction to overexposure in the online communication world. This overexposure has been exacerbated by online social networks, a development that courts have not been able to ignore. The dilemma presented by the transition to greater digital engagement is whether access to justice can be achieved in an open interactive Web 2.0 where human rights such as privacy are threatened.

The practical obscurity of paper records of the past has been revolutionised by the development of e-filing and digital records. The physical barrier for access to courtroom buildings has been transformed by virtual courtrooms which have the potential to provide open courts in a way not previously imagined. The use of video recordings, online transcripts, and instantaneous tweets has made disclosure of trial information a realistic expectation and an integral part of the process and procedures. They are for many an alternative method of accessing solutions to legal disputes whether these disputes reach final court hearings or are solved somewhere along the general pathway to dispute resolution.

It is now possible for litigants to select a digital pathway to justice. Banisar has claimed, '[i]n the 21st century, open justice should be online justice'.[558] In advocating 'proactive disclosure'[559] he considered that with the move to 'a more document-focused case system'[560] the rules need to change to enable anyone to access most documents electronically filed. The transition to the digital environment is transforming aspects of access to justice. Innovative technologies have presented a degree of transparency and openness that has confronted, and to some extent frustrated, the administration of justice by increasing the tension between open justice and privacy. Open access to courts, access to information and the reporting of court

[557] Beverly McLachlin, Chief Justice, 'Openness and the Rule of Law' (Paper presented at the Annual International Rule of Law Lecture, London, 8 January 2014).
[558] Banisar, above n 482, 57.
[559] Ibid 58.
[560] Ibid 57.

proceedings are rights which have become more negotiable online. I will explore the issues raised by the exposure of personal information online and the complexities online privacy in the following chapter.

.

Chapter Three – The exposure of personal information online – limiting access?

3.1 Introduction

The exposure of personal information online by the development of a digital pathway to justice in the infosphere[561] is an intangible cost which has not been the subject of extensive research. To understand the impact of the online exposure of such information and the tension between access and privacy, I will explore the nature of privacy and the necessity for a reformulation of the concept in the search for a new equilibrium.

By litigating, people are often obliged to make their personal information available for public scrutiny, although, the information is necessary to comply with the principle of open justice. When the digital pathway to justice is available for parties, access and openness are facilitated, however, even more data is thereby added to the online digital collection, available for aggregation, analysis and profiling. Access to information and the free flow of information presents opportunities for the courts, particularly for access to justice, however the economic value of this information in the market place and the difficulties of controlling its distribution poses considerable risks for privacy. This has accentuated a fundamental tension between access and privacy which is not only problematic to resolve but which questions the extent of access and openness that can be facilitated by Web 2.0 applications.

Disclosure of personal information is an essential element of participation in the interactive web. It is generally a defining characteristic of OSNs such as Twitter and Facebook. Such disclosure has created tension between the openness, made possible by new technologies, and the protection of personal information. It is apparent in the legal domain when electronic documents and vast collections of digital material are made available online in an accessible and permanent form.

The interrelationship between access to justice, the online exposure of personal data and privacy is complex. Soltani has explained that '[t]he technical underpinnings of our digital interactions are so complex that the average internet user doesn't have the know-how to build their own

[561] Luciano Floridi, 'The ontological interpretation of informational privacy' 7(4) *Ethics and Information Technology* 185-200, 188. The 'infosphere' described as the informational environment where the ontological features determine a specific degree of 'ontological friction' which regulates the flow of information within the system.

tools to browse the web, much less to interact securely and privately online'.[562] Legislative provisions concerning anonymity, pseudonyms, confidentiality and suppression orders aim to provide protection for privacy within the formal justice system, although digital access has presented more opportunities for invasion of privacy, at times limiting the effectiveness of these regulations.[563]

This analysis will begin by exploring the increased tension between access and privacy in the digital environment. I will then delineate the ambit of personal information and privacy as concepts. I will refer to the privacy literature that has identified common characteristics, particularly the characteristics relevant in the context of online access to justice and discuss the contrasting views of privacy, to determine whether a reformulation of privacy as a concept may provide some resolution of the tension between access and privacy.

3.2 Increased tension between access and privacy

3.2.1 The digital difference

The tension between privacy and the openness provided by Web 2.0 technologies, presents one of the greatest challenges for access to justice and the regulatory environment; a digital environment 'where personal data is continuously collected, enriched, amended, exchanged and reused'.[564] This tension has increased with the development of Web 2.0 due particularly to the vast quantities of personal data disclosed and accessible globally. Boundaries between nations, personal boundaries and traditional boundaries between government and society have been blurred by recent technological developments. As Spiecker[565] has observed, '[o]nline data

[562] Ashkan Soltani, 'The Privacy Puzzle: Little or No Choice', 81-82, 81 in *Internet Monitor 2013: Reflections on the Digital World* (Research Publication, No 2013-27, The Berkman Center for Internet & Society at Harvard University December 11, 2013) <https://cyber.harvard.edu/research/internet_monitor/paper_series>.

[563] Wide powers are provided by s 155 of the *Competition and Consumer Act 2010* (Cth), for example, to enable the Australian Competition and Consumer Commission to obtain information, documents and evidence to investigate possible contraventions of the Act. Oral examination is required to be held in private, in the exercise of investigative powers to determine whether a contravention has occurred. This is not stated explicitly in the Act but it has been found that where there is a clear legislative intention that the privacy of witness and anyone suspected of contravention would be protected for the purpose of the examination, the investigator may proceed in private: see Justice Jenkinson *Constantine v Trade Practices Commission* (1994) 48 FCR 141, 146-147.

[564] N Robinson et al, 'Review of the European Data Protection Directive' RAND Europe Report (May 2009) prepared for the Information Commissioner's Office UK, 7.

[565] Indra Spiecker genannt Döhmann, 'The European Approach towards Data Protection in a Globalized World of Data Transfer' Vol 9 in *Media Convergence: Perspectives on Privacy,* Dieter Dorr and Russell Weaver (eds) (de Gruyter, 2014).

processing operations are necessarily transnational, even global in nature'[566] and the handling of information 'an increasingly transnational activity'"[567]

Apart from Web 2.0 applications, there is an extraordinary variety of technologies which have the capacity to expose personal data on the internet. Monitoring of everyday life and every interaction is now possible. Jerry Kang considered that people were 'invisibly stamped with a bar code as soon as you venture outside your home'.[568] In the world of 'dataveillance',[569] such technologies as closed circuit television, systems for tracking mobile phones, 'intelligent transportation systems',[570] authorized wiretapping, use of globally unique identifiers in software,[571], passive millimeter wave imaging, 'BodySearch' and the possible use of 'ubiquitous miniature sensors floating in around in the air'[572] have the potential to seriously threaten personal privacy. More recently, the Electronic Frontier Foundation (EFF) has expressed concern about the way in which surveillance drones can be used by police in the US.[573]

Pre-installed applications[574] on smart phones have been identified as yet another threat to privacy. These applications enable some mobile phone manufacturers to gain additional profits by collecting person data through the use of malicious code and which is sold to third parties. The use of facial recognition software has more recently caused concern because it can be used to link photographs especially on OSNs to identities. This can be done by a third party without

[566] Ibid 46.
[567] Ibid 48.
[568] Jerry Kang, 'Information Privacy in Cyberspace Transactions', (1998) 50 *Stanford Law Review* 1193-1294, 1294.
[569] Roger Clarke, 'Introduction to Dataveillance and Information Privacy, and Definitions of Terms' (Original, 15 August 1997, revised 24 July 2016). In this article 'dataveillance' is defined by Clarke as 'the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons' <http://www.rogerclarke.com/DV/Intro.html>.
[570] A. Michael Froomkin, 'The Death of Privacy?' (2000) 52 *Stanford Law Review* 1461-1543, 1481. These systems provide continuous, real-time information regarding the location of traffic.
[571] The GUID is embedded in hardware and makes it possible to trace the author of documents.
[572] Froomkin, above n 570, 1500-1501.
[573] Shahid Buttar, 'DHS Issues Process and Privacy Guidance on State and Local Drones' (6 January 2016) Electronic Frontier Foundation <http://eff.org>. This article analyses the guidance issued by the Department of Homeland Security (DHS) working group on the use of drone aircraft and addresses the concerns over the use of such technological tools and the abuse that can result without 'rigorous controls and oversight embedded in code'.
[574] These are often referred to as apps, to distinguish them from web-based applications. There was initially a 'sharp divide between "native" applications, those that run entirely on the mobile device, and web applications' although this has changed as mobile applications have become more complex and serve 'more business-critical uses' rather than 'inexpensive recreational applications': see Anthony I Wasserman, 'Software Engineering Issues for Mobile Application Development' (Paper presented at the Workshop on Mobile Software Engineering, Santa Clara, 28 October 2010) (online) <http://www.mobileworkshop.org>.

the knowledge of the person photographed.[575]

Search engines are also seen as a threat to privacy. The increasing amount of personal data flowing across Web 2.0 is incorporated into the powerful search engines providing them with considerable control. They have been referred to as Search 2.0 by Zimmer.[576] This Search 2.0 is the 'combining of Google's suite of information-seeking products with Web 2.0 infrastructure' and is useful in providing more useful information for users and often predicting what users need, however it also involves the aggregation of data and monitoring of users' activities and so threatens informational privacy. Zimmer considers that the 'deterioration of "privacy via obscurity" in online personal data' and the concentration of surveillance by a few powerful financially motivated search engines is a problem for Web 2.0. Users are subjected to 'a robust infrastructure of dataveillance'.[577]

The vast quantities of information available in the digital age, sometimes referred to as big data,[578] have been considered to raise 'the risk of unauthorized access to information and subsequent privacy violations'.[579] Masiello and Whitten considered that 'once recorded, information can too easily be intentionally or accidentally reapportioned in ways that violated the privacy of the subject'.[580] This raises the issue of whether access to justice online will enhance or diminish the access so well facilitated by innovative technologies.

The enormous volume of data[581] created digitally online that has been viewed as challenging privacy by casting 'doubt on the distinction between personal and non-personal data', clashing

[575] James Manning, 'Face up to social reality' *The Sydney Morning Herald* (online) 10 June 2012. This software tags photos and identifies users. <http://www.smh.com.au/digital-life/consumer-security/face-up-to-social-reality-20120609-2027x.html>.
[576] Michael Zimmer, 'The Externalities of Search 2.0: The Emerging Privacy Threats when the Drive for the Perfect Search Engine meets Web 2.0', 13(3) *First Monday* (online) 3 March 2008, <http://dx.doi.org/10.5210/fm.v13i3.2136>.
[577] Ibid.
[578] Sunil Erevelles, Nobuyuki Fukawa and Linda Swayne, 'Big Data consumer analytics and the transformation of marketing' (2016) 69 *Journal of Business Research* 897-904.
[579] Betsy Masiello and Alma Witten, 'Engineering Privacy in an Age of Information Abundance' (Paper presented at the Association for the Advancement of Artificial Intelligence Spring Symposium Series, Palo, Alto, 22-24 March 2010) <www.aaai.org/ocs/index.php/SSS/SSS10/paper/view/1188> 119-124, 120.
[580] Ibid 121.
[581] James Manyika et al, 'Big data: The next frontier for innovation, competition, and productivity' (Report, McKinsey Global Institute, May 2011). The report estimated that 'new data stored by enterprises exceeded 7 exabytes of data globally in 2010 (15) and that new data stored by consumers around the world that year exceeded an additional 6 exabytes,15. YouTube was reported as a 'hugely significant data aggregator', with visitors to the site spending more than 2.9 billion hours on the site each month (21) <http://www.mckinsey.com>.

'with data minimization' and undermining 'informed choice'.[582] Paradoxically, the accumulation of such huge data bases of personal information has only been made possible by the facilitation of access accompanying innovative technologies. The 'unprecedented volume, velocity, and variety of primary data' available from consumers has been considered to be 'a new form of capital in today's marketplace'. By using consumer analytics hidden insights about consumers can be extracted and exploited, turning 'the average consumer into an incessant generator of both traditional, structured, transactional data as well as more contemporary, unstructured, behavioural data'.[583]

Such big data manipulation has been referred to as 'data mining on steroids'[584] and 'unthinkably intrusive and eerily omniscient',[585] due to the overwhelming size of the datasets which require the use of 'new computational frameworks for storing and analysis'.[586] According to Boyd and Crawford,[587] big data refers to very large data sets, the tools and 'procedures used to manipulate and analyse them, and to a *computational turn*' which has created 'a radical shift in how we think about research' and 'how we should engage with information'. It has been viewed as challenging the very foundations of privacy laws because it enables re-identification of data subjects using non-personal data, weakening anonymisation and exacerbating harm to individual dignity by collecting private data on a massive scale.[588] It makes aggregation 'more granula, more revealing, and more invasive'. The virtual explosion of communication has created big data which consists of huge interlinked data sets which Boyd has found closely intermingled with privacy issues. For Rubinstein, '[p]rivacy will never be encoded in zeros and ones. It will always be a process that people are navigating', so despite the link between data and personal identity, the protection of personal information will remain a matter of discourse. It is also no longer intrusion by the media, governments or commercial enterprises alone that threaten privacy but self-disclosure.

Richards and King[589] have proposed a big data ethics to ensure there is 'privacy, transparency,

[582] Ira S Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' Public Law & Legal Theory Research Paper Series Working Paper No 12-56 (online), October 2012 <http://ssrn.com> 1-14, 1.
[583] Ibid 897-898.
[584] Ibid 3; see also, Julie E Cohen, 'What Privacy is For' (2013) 126 *Harvard Law Review* 1904, 1921.
[585] Julie E Cohen, 'What Privacy is For' (2013) 126 *Harvard Law Review* 1904, 1921.
[586] Rubinstein, above n 568.
[587] danah boyd and Kate Crawford, 'Six Provocations for Big Data' (Paper presented at Oxford Internet Institute conference, *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society,* September 21, 2011) <http://ssrn.com> 3.
[588] Rubinstein, above n 582, 4.
[589] Neil M Richards and Jonathan H King, 'Three Paradoxes of Big Data' (2013) *Stanford Law Review Online* 41.

autonomy, and identity protections' and an understanding of the appropriate context for big data analytics.[590] They were concerned about three paradoxes in relation to big data: Transparency, Identity and Power. The first: the Transparency Paradox concerns the promise of benefits from increased transparency, however the data is collected invisibly by 'opaque' tools in secret by 'unreviewable decision-makers'. The Identity Paradox concerns the conflict between an individual's desire for control over personal identity which is threatened by big data. Without protection the information collected can be used to restrict identity.[591] The Power Paradox was seen in the benefit which most likely will be gained by institutions who are mining, analysing and sorting the individual's data.

While recognising the social and economic benefits of big data, Tene and Poetsky also expressed concern at the unique privacy risks.[592] The risks were seen as resulting from the incremental effect of the accumulation of personal data and linking of any piece of data to a person's real identity; the automated decision-making based on algorithms and artificial intelligence which was seen as creating opaque profiles compartmentalising society;[593] the predictive analysis emanating from big data was seen as useful in such fields as 'law enforcement, national security, credit screening, insurance and employment', however, it could lead to 'morally contentious conclusions' and stifle individuals and society;[594] the lack of access and exclusion of individuals from their data which favours governments and big business; the risk that data analytics could 'cross the threshold of unethical behaviour';[595] and also of concern was the risk of the chilling effect of tracking information in a 'surveillance society'. They concluded that a legal model should be developed which could share the benefits of data with both individuals and organisations, providing access and transparency for individuals.[596]

Ohm also warned about the incremental effect of accumulated data which becomes more and more revealing, particularly when linked to an individual and can lead to an erosion of privacy when the individual's profile is exposed.[597]. According to Ohm, '[d]ata can be either useful or

[590] Ibid 46.
[591] Ibid 44.
[592] Omer Tene and Jules Polonetsky, 'Big Data for All: Privacy and User Control in the Age of Analytics' (2013) 11 *Northwestern Journal of Technology and Intellectual Property* 239-273.
[593] Ibid 252.
[594] Ibid 253.
[595] Ibid 256.
[596] Ibid 272-273.
[597] Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 *University of California, Los Angeles* 1701-1777.

perfectly anonymous but never both'.[598] Despite the removal of revealing data fields, identity can be unlocked by the discovery 'of surprising uniqueness remaining in the data'.[599] Ohm asserted that nearly everyone can be 'linked to at least one fact in a computer database that an adversary could use for blackmail, discrimination, harassment, or financial or identity theft', the 'hypothetical database of ruin' which has been created by reidentification.[600] Reidentification science was considered by Ohm as exposing the underlying promise made by privacy laws 'that anonymization protects privacy'.[601] It also has the capacity to make laws, such as the EU Data Protection Directive[602] overbroad as it relies on direct or indirect linking to a person, and laws such as those in the US that rely on personally identifiable information too narrow, allowing 'entire industries to escape privacy regulation completely'.[603] His solution, based on Nissenbaum's contextual integrity,[604] was to solve the problems created by easy reidentification by the creation of 'a combination of comprehensive data-protection regulation and targeted, enhanced obligations for specific sectors' as well as a 'sea change in the law'.[605] He revealed that there has been a fundamental misunderstanding about the effectiveness of procedures such as deleting personal identifies and modifying categories of information that are identifiers in the face of reidentification which can 'create and amplify privacy harms' by combining databases that should be kept separate.

The digital difference recognised by Floridi is that 'new ICTs [information and communication technologies] have re-ontologized the infosphere'.[606] Floridi viewed digital technologies as radically different from old technologies because they have changed the very nature of the environment, they have changed the participants, they have changed interactions and they 'can

[598] Ibid, 1704
[599] Ibid 1723.
[600] Ibid 1746-1748.
[601] Ibid 1704.
[602] This refers to the EU Directive 95/46/EC <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>.
[603] Tene and Polonetsky, above n 592, 1762.
[604] Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 *Washington Law Review* 119-157.
[605] Ibid 1763.
[606] Floridi, above n 547, 188. The 'infosphere' described as the informational environment where the ontological features determine a specific degree of 'ontological friction' which regulates the flow of information within the system. What Floridi finds different is the influence of the new technologies due to five factors: 'The digitization of the information environment' with the transition from analogue to digital data; '"The homogenization of the processor and the processed' as digital resources and digital tools converge; 'The evolution of new informational agents' which includes artificial and hybrid agents (referring to people equipped with such artificial devices as digital cameras, laptops and smart phones; 'the informationalization of interactions' which occurs 'where there is no ontological difference between processors and processed, interactions become equally digital'; and 'The mutation of old agents into informational agents' or the 'migration of humanity from its *Umwelt* to the infosphere'.

dramatically change the conditions of possibility of informational privacy'.[607] The digital ICTs are not merely enhancing technologies but are revolutionary in an ontological way because 'they engineer environments that the user is then enable to enter through (possibly friendly) gateways' causing 'an epochal, unprecedented' transformation of human into 'informational entities'.[608] In the Christensen interpretation, as discussed in Chapter One, these digital technologies are no longer just sustaining but disruptive technologies.

3.2.2 The distinction between public and private information

The online exposure of personal information has transformed any clear distinction that may have existed between what is public and what is private, to the extent that some authors refer to information that is 'publicly private' or 'privately public' online.[609] Whether information is public or private has become more relative to context, intention and time. This has significance for the nature of personal data, particularly in the context of digital access to justice. What may be considered public in one context and at one time may not be public in another context. Information disclosed in the context of bankruptcy proceedings, for example, would not necessarily be considered public data in the event of discharge of bankruptcy.

What were previously private spaces or even '*private* public spaces'[610] have been transformed into '*public* public *spaces'* and have imposed 'press conference behaviour' on people.[611] Abril[612] found that the traditional view of privacy in the online 'spaceless world' and 'the law's reliance on spatial linchpins' were inadequate.[613] She considered that the architecture of the internet blurs the line between private and public. The courts however have relied on 'absolutist statements' to find that there is no privacy in public spaces. Abril considered that there could be privacy 'where there is no physical space and no inherently private subject matter, secrecy, or seclusion'.[614] The concept of physical space should be discarded for consideration of 'walls of confidentiality built by technical architecture, agreements, and relational bonds'. The subject matter should be considered in terms of 'its overall accessibility' with a focus on the 'contextual

[607] Ibid.
[608] Ibid, 188-190.
[609] Patricia G Lange, 'Publicly Private and Privately Public: Social Networking on YouTube', 13 *Journal of Computer-Mediated Communications* 361-380.
[610] Jeffrey Rosen, 'The Eroded Self' *New York Time* (online) 30 April 2000) <http://people.brandeis.edu/~teuber/rosen1.html> 84.
[611] Ibid 85.
[612] Patricia Sánchez Abril, 'Recasting Privacy Torts in a Spaceless World' (2007) 21 *Harvard Journal of Law & Technology* 1-48.
[613] Ibid 17-20.
[614] Ibid 47.

analysis of the harm' from disclosure.[615]

Previously public expression did not mean instant communication to the world and it was more often 'transitory' in nature. Consumers in the digital area were seen as gaining a voice in the open market, but only by voluntary disclosure.[616] Kenyon and Richardson have expressed greater concern for privacy over networks which cross national boundaries and where data is stored and retained for long periods of time.[617] The development of a globalised network society where personal data is constantly being disclosed,[618] collected and aggregated, particularly in OSNs, has created an exposed information environment demanding well considered data regulations. This personal data has been referred to as the 'currency of the internet economy'.[619] More recently, the widespread use of OSNs and the 'unprecedented readiness' for people 'to expose even the most private data'[620] has, according to some authors, made self-regulation an unacceptable alternative to government legislation and has made 'the necessity to define and ensure the constitutive elements of privacy' an imperative[621]. Self-disclosure has become a feature of the internet, particularly for participation in OSNs. It is necessary for participation in many aspects of digital life, whether to gain access to government services or for social inclusion. It illustrates the new dynamics of digital privacy and the need for reconceptualising privacy.

The feeling of comfort provided to users about publishing their private data on social networks was attributed to the illusion of privacy and control particularly in 'blurry-edged' social networks.[622] Gelman questions whether the law should consider some disclosures on the

[615] Ibid.
[616] Ibid.
[617] Andrew T Kenyon and Megan Richardson, 'New dimensions in privacy: Communications technologies, media practices and law', Chapter 1 in Andrew T Kenyon and Megan Richardson (eds) *New dimensions in privacy: International and Comparative Perspectives*, (Cambridge University Press, 2010).
[618] Information Society & Media and Joint Research Centre, *Special Eurobarometer 359*: *Attitudes on Data Protection and Electronic Identity in the European Union*, (June 2011). This report found that, '74% of the Europeans see *disclosing personal information* as an increasing part of modern life'.
<http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf> Executive Summary, 1.
[619] Angel Gurría, 'Closing remarks by Angel Gurría, OECD Ministerial Meeting on the Future of the Internet Economy', (Speech delivered at the OECD Ministerial Meeting on the Future of the Internet Economy, Seoul, 18 June 2008)
<http://www.oecd.org/korea/closingremarksbyangelgurriaoecdministerialmeetingonthefutureoftheinternetecono my.htm>.
[620] Spiros Simitis, 'Privacy – An Endless Debate" (2010) 98 *California Law Review* 1989-2010, 2004.
[621] Ibid.
[622] L Gelman, 'Privacy, Free Speech, and "Blurry-Edged" Social Networks' (2009) 50 *Boston College Law Review* 1315-1344. The 'blurry edge' referred to by Lauren Gelman is the undefined social network resulting from the inability of users to be able to identify everyone in their social network.

internet as intended for a limited audience. Social networks like Facebook are seen as creating an 'aura of privacy'[623] because they are designed to encourage users to disclose information, to link to friends, upload photos, identify and tag, and add comments. While there are privacy controls, users either do not apply them or they were unaware of the extent they could control their personal data.[624] At the same time such social networks encourage users to disclose as much as possible. Gelman concluded that if Web 2.0 applications are to be used more privacy tools need to be provided as well as changes in privacy law to ensure protection for speech and privacy.

The shifting boundaries of public and private life have been conceptualised as a 'contested terrain' in 'a new kind of information war' where there is 'constant negotiation and struggle'.[625] Public and private as seen as no longer attached to physical boundaries but are 'spheres of information and symbolic content' in the era of new media. Privacy in public places has been found to be more difficult to analyse than when considering privacy behind closed doors in what is traditionally considered a private place.[626] The issue considered in the analysis was whether there should be a legal right to privacy in public places, and in what circumstances this right should exist, or whether industry codes of practice and rules would be sufficient to provide protection. Hickford refers to the findings of Moreham that, '[p]eople should be presumed to have a reasonable expectation of privacy if they are involuntarily experiencing an intimate or traumatic experience in public, they are in a place in which they reasonably believe themselves to be imperceptible to others' or technological devises were used to penetrate 'self-protection barriers', such a clothing.[627]

The blurred boundaries between public and private spaces were discussed in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd*:

> There is no bright line which can be drawn between what is private and what is not. Use of the term 'public' is often a convenient method of contrast, but there is a large area in between what is necessarily public and what is necessarily private. An activity is not private simply because it is not done in public. It does not suffice to make an act private that, because it occurs on private property, it has such measure of protection from the public gaze as the characteristics of the property, the nature of the activity, the locality, and the disposition of the property owner combine to afford. Certain kinds of information about a person, such as information relating to health, personal

[623] Ibid.
[624] Ibid 1328.
[625] John B Thompson, 'Shifting Boundaries of Public and Private Life' (2011) 28 *Theory, Culture & Society*, 49 – 70.
[626] NZLC MP19, *A Conceptual Approach to Privacy: Miscellaneous Paper* (Wellington, New Zealand, October 2007) <http://www.lawcom.govt.nz>.
[627] Ibid.

> 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 to a reasonable person of ordinary sensibilities is in many circumstances a useful practical test of what is private.[628]

Chief Justice Gleeson acknowledged that everything done by a landowner is not a private act, nor is it private because the landowner would prefer the act was not observed. It could be a public act even if performed on private property. His Honour discussed the nature of 'private in a proprietorial sense' and considered that by virtue of the exclusive possession of premises, the respondent could refuse permission for anyone to record its operations.

Lange, in an analysis of YouTube[629] has viewed communication technologies as 'eroding the boundaries between "publicity" and "privacy" in fundamental ways'.[630] She analysed the way in which 'YouTube participants developed and maintained social networks by manipulating physical and interpretive access to their videos'.[631] Lange found that there were more than strictly public and strictly private interactions on YouTube and some participants were shown to demonstrate 'publicly private' behaviour, where the identity of the video maker was revealed but the content relatively private, and others 'privately public' behaviour where the content was shared widely and the detailed information about the video maker limited. Lange concluded that 'people will likely continue to seek ways to carve out privacy in highly visible media environments', despite increasing surveillance by manipulating public systems to preserve different levels of 'informational and behavioral publicity and privacy'.[632] She considered that the use of social network sites could be optimised if technical features could be used to assist control and customisation for public and private interaction. Although, despite security protections employed by the legal system for their online data, individuals disclose so much information that it is difficult for 'the average internet user to find a reasonable and effective

[628] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 226 [42]. This case the appellant sought an order to discharge an interlocutory injunction which prevented the Australian Broadcasting Corporation from, amongst other things, broadcasting a video tape of possums being stunned and killed in the respondent's abattoir. It had been taken by an unknown trespasser using secret cameras. In allowing the appeal, the Court held that the interlocutory injunction could only be granted to protect a legal or equitable right when there was an underlying case of action. In this case it was held that the corporation, the abattoir, could not suffer any mental distress similar to a natural person, although may suffer a loss of income.

[629] YouTube is a public internet site where people can share videos or view the videos submitted by others <http://www.youtube.com>.

[630] Patricia G Lange, 'Publicly Private and Privately Public: Social Networking on YouTube', (2007) 13 *Journal of Computer-Mediated Communications* 361-380.

[631] Ibid 361.

[632] Ibid 378.

way to protect' private information.

As Simitis has asked, 'Can a legally guaranteed respect for privacy be upheld in a society in which technology incites and sustains a constant disclosure of highly private data?'[633] As Schauer[634] has reasoned, recent technological developments have 'changed our very conception of privacy itself' by the increasing pervasiveness which informs 'society's general understandings of database privacy'.[635] Schauer reasoned that the normative idea of privacy should be more important, so that we should be considering what personal data 'people *ought* to be allowed to protect' rather than focusing on what people expect to be protected.[636]

The conflict between gaining access to online services and the protection of privacy has not found a resolution in current privacy laws or regulations. The greater transparency and openness provided by the availability of information online has led to unprecedented disclosure of personal information, adding uncertainty to the distinction between what is private and what is public. Providing access to justice in the digital era has highlighted a number of privacy related issues. The development of many e-Government initiatives and the commercialisation of the internet, together with enabling technologies, have resulted in growth of huge data sets, subject to surveillance. The digital era has had a considerable transformative impact on the nature of privacy and personal information. I will analyse the literature on privacy and suggest that an ontological interpretation of informational privacy may assist in resolving the tension between online access and privacy.

3.3 Delineating the ambit of privacy and personal information

3.3.1 Introduction

Due to the increasing tension between open access and privacy in the digital era and a blurring of boundaries between what is public and what is private, it is necessary to determine the scope of the data that is at risk, determining whether 'privacy' as a concept can be defined or whether more clarity can be reached by isolating characteristics of the concepts. A substantial body of work has focussed on the function of privacy and personal data and the role of context and control in clarifying their ambit.

[633] Ibid.
[634] Frederick Schauer, 'Internet Privacy and The Public-Private Distinction' (1998) 38 *Jurismetrics* 555-564.
[635] Ibid 556.
[636] Ibid 564.

3.3.2 Privacy: a definable concept?

The difficulties faced in defining 'privacy' have been alleged to be due to 'conceptual-stretching' and the 'range of empirical referents or observables' that the concept encompasses.[637] It has been described as so dynamic that whatever solutions are found suitable today may be 'unacceptable or ineffectual' in the future.[638] Regan considered that 'finding a perfect conceptualization of the value [of privacy] may distract us from developing and analysing options for responding to the problems involved'[639].

The development of new technologies has had considerable impact on the formulation of 'privacy' as a concept and the search for protection. In response to intrusive reporting of personal information due to technological developments in photography, the media were considered by Warren and Brandeis in 1890 to 'have invaded the sacred precincts of private and domestic life'.[640] Warren and Brandeis demanded protection for privacy to prevent new technologies invading private life and affecting the 'inviolate personality' of individuals, as well as society as a whole.[641] They reasoned that the right to privacy was a new general right of the individual to be 'let alone'.[642] Solitude and privacy were viewed as more essential in a world of greater intensity and complexity, so that it had become necessary to recognise new rights under the common law. Warren and Brandeis referred to the right to privacy under French law, distinguishing their argument that protection is sought for 'injury to the right of privacy' not for 'injury to the individual's character'.[643] It was the individual who was seen as responsible for any acts and omissions, "[i]f he condones what he reprobates, with a weapon at hand equal to his defence, he is responsible for the results."[644] Self-disclosure was considered a factor in limiting privacy so that '[t]he right to privacy ceases upon the publication of the facts by the individual, or with his consent'.[645]

---

[637] Colin J Bennett, 'In Defence of Privacy: The concept and the regime' (2011) 8 *Surveillance & Society* 485-516, 493.
[638] Malcolm Crompton: 'What is Privacy?' A paper delivered by the Australian Federal Privacy Commissioner at the Privacy and Security in the Information Age Conference, 16-17 August 2001, Melbourne, 3.
[639] Bennett, above n 637, 498.
[640] Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193-220, 195. There has been some speculation in the past about the reasons that this article was written. William Prosser attributed the article to the irritation felt by the Warrens to personal and embarrassing publicity by local newspapers on the occasion of their daughter's marriage: see William L Prosser, 'Privacy' (1960) 48 *California Law Review* 383-423. Dorothy J Glancy, 'The Invention of the Right to Privacy' (1979) 21 *Arizona Law Review* 1-39. Glancy, while agreeing that the invasion of social privacy by newspapers was the catalyst for the article, she considered that they had other motives such as the desire to produce new and interesting copy for the *Harvard Law Review* and to promote the new firm, Warren & Brandeis as widely as possible.
[641] Ibid 205.
[642] Ibid.
[643] Ibid 214.
[644] Ibid 290.
[645] Ibid 218.

Although the right to privacy has been acknowledged in international documents that define human rights, such as the *Universal Declaration of Human Rights*,[646] the *International Covenant on Civil and Political Rights*,[647] the *European Convention on Human Rights*,[648] and the *Charter of Fundamental Rights of the European Union*[649] however, these documents contain no definition of 'privacy'. Definitions of 'personal information'[650] and 'personal data'[651] are more common. The latter term has been used more specifically in an electronic context.

A leading authority on privacy, Clarke, considered that privacy is 'the interest that individual have in sustaining a 'person space', free from interference by other people and organisations'.[652] He commented, however, that privacy is an 'abstract and contentious notion'[653] that has multiple dimensions[654]. In a broad sense it can encompass privacy of the person or *"bodily privacy"*,[655]

[646] Privacy was recognized by the United Nations in 1948 by Article 12: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

[647] This entered into force generally on 23 March 1976. Article 17 states: "(1) No-one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his home and reputation. (2) Everyone has the right to the protection of the law against such interference or attacks." This Declaration was signed by Australia on 18 December 1972 and ratified on 13 August 1980.

[648] This came into force on 3 September 1953 and has been subsequently amended by protocols, most recently No 14 which came into force 1 June 2010. Article 8 provides: "1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and I necessary in a democratic society in the interest of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedom of others."

[649] The Treaty of Lisbon gave full legal effect to this Charter on 1 December 2009. Article 7 provides: "Everyone has the right to respect for his or her private and family life, home and communications."

[650] Section 6 *Privacy Act 1988* (Cth) "*personal information* means information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not." This definition was amended in 2014. The meaning of personal information is extended in s 187LA of the *Telecommunications (Interception and Access) Act 1979* (Cth) to cover information kept under Part5-1A of that Act:

[651] The *Data Protection Act 1998* (UK) refers to "data" as information processed automatically or non-automatically within a filing system; "personal data" is data that relates to an identifiable individual and is the same as the definition in Article 2 of the EU Directive. Data in electronic form is defined in s 1(1)(a) of the DPA. Four types of data are referred to in the DPA: electronic data; data forming part of a relevant filing system; data forming part of an accessible record; and data recorded by a public authority.

[652] Clarke, above n 569.

[653] Ibid.

[654] Some authors refer to useful categories or concepts of privacy such as those outlined by the Electronic Privacy Information Center[654] and Privacy International[654] in *Privacy and Human Rights 2000: An International Survey of Privacy Law and Developments[654]*. These include: *information privacy* which is the collection and management of personal data or data protection; *bodily privacy* or the protection of a person's body from invasive procedures, searches and investigations; *communications privacy* including the security of communications; and *territorial privacy* concerning the limits on intrusion in public and private spaces.

[655] Clarke, above n 569. This concept has been more commonly seen as a human right and can extend to rights such as freedom from torture or more directly related to privacy by including such aspects as compulsory immunization.

privacy of personal behaviour or "media *privacy",*[656] privacy of personal communications or "*interception privacy"*[657] and privacy of personal data. The combination of personal communications and personal data can be referred to as *"information privacy"*.[658] It is information privacy[659] that Clarke sees as the target of most legislation. Clarke explains that privacy is important from a number of perspectives,[660] which are to some extent related and encompass a variety of human needs. The fulfilment of these needs allow people the freedom to behave, associate and innovate without the chilling effect of surveillance.

The difficulty in analysing the impact of interactive applications on the protection of privacy is the close connection between the terms 'privacy' and 'personal information'. They are not terms that are mutually exclusive but 'overlap' with considerable inconclusiveness and disconnection.[661] Privacy can be considered as an all-encompassing term whose meaning is continually evolving, almost impossible to define and contingent on moral values and context.[662] Personal data is commonly defined in privacy legislation.[663] It is a concept that was considered by an EU Working Party[664] which found that while a 'broad notion of personal data' was adopted in Directive 95/46/EC, four main elements could be identified which are 'closely

[656] Ibid. This includes sensitive information including religious practices and sexual preference.

[657] Ibid. This includes the freedom to communicate with other people and retain control free from such interference, interception and recording devices over the telephone.

[658] Ibid. This is data about individuals that they would wish to control.

[659] The *Privacy Act 1988* (Cth) Part 11, Division 1, s 6 provides that "***personal information*** means information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not".

[660] Clarke, above n 569. Clarke refers to philosophical, psychological, sociological and economic needs.

[661] Gloria Gonzalex Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer, 2014). Fuster considered that the EU fundamental right to personal data protection developed through the partial interchangeability of 'privacy' and 'personal data' as legal terms. In analyzing the use of the terms in the OECD Guidelines, Convention 108 and Directive 95/46/EC she found (257) that any laws on the processing of information about individuals 'serve primarily privacy (even if not only privacy) which makes them also somehow privacy laws. At the same time the word 'privacy' was held to refer to something different from personal data protection, specifically on the basis of Article 8 EU Charter, sometimes 'data protection' and 'personal data protection' being used as identical legal concepts but also different in reference to Convention 108 which refers particularly to rights and fundamental freedoms of individuals, specifically the right to privacy. Fuston referred to the decision in C-28/08 *P Commission v Bavarian Lager* [2010] ECR 1-6055, where a significant legal distinction between 'privacy' and privacy together with 'personal data protection'.

[662] Legal concepts are dependent on legal norms which are dependent on the interpretation of terms in authoritative documents and the pragmatics of the different situations in which the norms have to be applied. They cannot be expected to have a stable meaning. Giovannit Sartor et al (eds) *Approaches to Legal Ontologies: Theories, Domains, Methodologies* Law, Governance and Technology Series (Springer, 2011) 17-18.

[663] Section 6 of the *Privacy Act 1988* (Cth) provides: "'***personal information***" means information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion in true or not; and (b) whether the information or opinion is recorded in a material form or not.'

[664] Article 29 Data Protection Working Party 'Opinion 4/2007 on the concept of personal data', 01248/07/EN WP 136.

intertwined and feed on each other.'[665] It is privacy as it is related to personal data that is protected by the provisions of Article 23.1 of the General Data Protection Regulation (GDPR). This Article imposes an obligation on data controllers to provide protection of personal data at the design level.[666] It is a concept commonly used in connection with personal information online and can be defined with more precision than privacy. In the EU 'human dignity' has been identified as 'the fundamental concept that provides the framework' within which to interpret 'informational privacy' under the GDPR.[667]

Privacy has been seen as a primary component of moral understanding about technology and one most readily discussed, particularly in relation to the assessment of regulation of technologies.[668] It can be used to mark the limits of moral acceptability,[669] although with limited functionality in 'settling disputes over boundaries'.[670] In deploying interactive applications the existing moral concept and understanding of privacy has been 'stretched' to provide a regulatory framework which calls into question the legitimacy of the use of such applications.[671] The plurality of ethical and philosophical beliefs has created difficulties for the resolution of public policy and the formulation of privacy laws. It is the substantive legitimacy, or the concern for what decisions can be made in relation to the protection of personal data, that is central to a determination of privacy policy. As Brownsword and Goodwin have highlighted, '[p]erceptions of the moral legitimacy of regulatory instruments and regimes go therefore not only to the efficiency of the instruments themselves but to matters of social and political cohesion, and ultimately to the (self-) identity of the community itself'.[672]

Burdon and Telford considered that despite the absence of uniformity in defining privacy and classifying personal information, 'definitions of personal information are central to the application of most privacy laws' and the formulation of an effective response to privacy

[665] Ibid 25. The elements identified included: 'any information'; 'relating to'; 'identified or identifiable' and 'natural person'.
[666] Mireille Hildebrandt and Laura Tielemans, 'Data protection by design and technology neutral law' (2013) 29 *Computer Law & Security Review* 509-521, 517.
[667] Luciano Floridi, 'On Human Dignity as a Foundation for the Right to Privacy' (2016) 29(4) *Philosophy & Technology* 307-312 <http://link.springer.com/article/10.1007/s13347-016-0220-8>.
[668] Brownsword and Goodwin, above n 64, 223.
[669] Ibid 188.
[670] Ibid 245.
[671] Ibid 172.
[672] Ibid.

protection.[673] In order to determine what information can be regulated, a 'coherent conceptual basis of personal information'[674] is required which must be extracted from the diversity of views.

The validity of the search for a concise definition of 'privacy' is called into question by the extensive privacy literature that has failed. What appears to be a more valid search is for ways to address the essential issues that privacy raises and to find an effective response. Privacy is a concept that the literature reveals is relative, contextual, fragmented and, at times, elusive. However, it is a concept that remains of concern, particularly for regulation in the digital environment.[675] The concepts, 'personal information' and 'privacy' nevertheless require a conceptual framework adapted to the digital era of Web 2.0 and the highly dynamic nature of interactive applications which encourage data disclosure. I will first consider some of the essential issues raised by privacy identified in the literature, including, privacy-control paradigm, privacy as a context dependent concept, and privacy as identity. I will then analyse the benefits of Floridi's ontological interpretation of informational privacy for the digital era.

3.3.3 The essential issues

Wacks has suggested that to find 'a more rational, direct, and effective method of seeking to address the central questions of "privacy"' and a way of avoiding 'the conceptual labyrinth that has so far impaired their satisfactory resolution'[676] is to 'isolate the essential issues that give rise to such claims'.[677] He considered that the arguments about the meaning of the term 'frequently proceed from fundamentally different premises'; there is confusion about its 'instrumental and inherent value', and there is confusion between descriptive accounts and normative accounts.[678]

One of the issues that has been the subject of considerable analysis and which forms a substantial body of work in privacy literature is that of privacy as a control-related concept.[679] Altman analysed privacy as 'an interpersonal boundary control process'[680] and viewed it as a 'selective control of access to the self or to one's group', presenting a conceptual framework

[673] Mark Burdon and Paul Telford, 'The Conceptual Basis of Personal Information in Australian Privacy Law' (2010) 17(1) *eLaw Journal: Murdoch University Electronic Journal of Law* 1.
[674] Ibid.
[675] Daniel J Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York University Press, 2004).
[676] Raymond Wacks, *Privacy and Media Freedom* (Oxford University Press, 2013) 12.
[677] Ibid 9.
[678] Ibid 11.
[679] See: Alan F Westin, *Privacy and Freedom* (1967); Charles Fried, 'Privacy' (1967-1968) 77 *Yale Law Journal* 475-493; Irwin Altman, 'Privacy Regulation: Culturally Universal or Culturally Specific?' (1977) 33 *Journal of Social Issues* 66-84.
[680] Irwin Altman, 'Privacy: "A Conceptual Analysis"' (1976) 8 *Environment and Behavior* 7-29, 7.

based on key elements of privacy.[681] Altman's analysis emphasised features of privacy such as the different privacy dynamics for various social units, the 'shifting dialectic process'[682] involved with people wanting openness at time and not at others; 'the flexible barrier or boundary between the self and nonself'.[683] He explored the concept as discussed in several disciplines such as psychology, sociology, anthropology and law to distinguish these elements. Altman considered the regulation of these boundaries was a dynamic process with 'continual adjustment and readjustment as new situations emerge, as personal and group motivations shift …'[684] Westin's views[685] were central to Altman's framework with privacy seen as a 'shifting dialectic process', suggesting that people seek to balance 'openness and closedness'.[686]

Westin also considered privacy to be concerned with the ability to control how much people reveal to others.[687] He analysed the role of privacy norms in the context of political, socio-cultural and personal settings with four states of privacy – solitude, intimacy, anonymity and reserve.[688] He considered it was a concept that concerned issues of 'values, interests and power'.[689] Much of his analysis was based on survey research between 1978 and 2003 which he did with Louis Harris in which he identified a diversity of concerns about privacy driven by new technologies, public attitudes and 'organizational policies and law'.[690]

For Fried, privacy was an 'object of considerable concern'[691] and urgency because of 'insidious intrusions of increasingly sophisticated scientific devices into previously untouched areas'.[692] It was a concept 'implicated in the notions of respect and self-respect, and of love, friendship and

[681] Ibid 8.
[682] Ibid 12.
[683] Ibid 13.
[684] Ibid 23.
[685] Ibid 7-8.
[686] Ibid 13.
[687] Alan F Westin, *Privacy and Freedom* (Athenum, 1967).
[688] Alan F Westin, 'Social and Political Dimensions of Privacy' (2003) 59 *Journal of Social Issues*, 431-453, 3.
[689] A Munir and S Yasin, *Privacy and Data Protection: A Comparative Analysis with Special Reference to the Malaysian Proposed Law* (Sweet & Maxwell, 2002), 2.
[690] Westin, above n 676. In this article, Westin identified three phases of contemporary privacy development: the first era (1961-1979) where Americans considered that privacy was essentially 'in good shape'; the second era (1980-1989 of advancing technological change with a 'flood of writings about privacy', however 'a period of relative calm before the storm'; and the third era (1990-2002) when privacy became a 'first-level social and political issue' with a steady increase in public concern over privacy. Westin reported that in early 2002 87% of internet users were still concerned about privacy threats. He concluded that privacy issues permeated many facets of life, key relationships, politics and culture.
[691] Charles Fried, 'Privacy' (1968) 77 *Yale Law Journal* 475-493.
[692] Ibid 475.

trust'.[693] Fried considered that the 'control' of information about ourselves is the very basis of privacy and this is an aspect of 'personal liberty'. Legal rules were viewed as important in 'establishing the social context of privacy' not just to protect privacy but as 'an essential element' so that people not only have control over information about themselves but there is 'a feeling of security in control over that information'.[694]

This broad or unitary definition of privacy was criticized by Lusky[695] as oversimplified[696] and in need of ongoing qualification because it was viewed as a definition which hindered the development of 'comprehensive remedies'.[697] Lusky also criticised the 'balancing' solution to privacy problems such as the balance between disclosing private information and keeping some information private, feeling free to decide who has to know this information and when and under what conditions it would be disclosed. Lusky distinguished between information which is objectionable because it is false and misleading and information, while accurate and complete, cannot be disclosed. Therefore for him the solution is 'delineation of forbidden areas'.[698] The analysis that he considers necessary is the determination of whether particular information has negligible social utility and whether it can be 'demarcated with sufficient clarity to avoid the danger that a prohibition will discourage other more useful communication".[699]

Schwartz identified what he saw as 'the flaws in the leading paradigm of information privacy',[700] that is the interpretation of privacy as a personal right to control information about oneself. He viewed information privacy as a 'constitutive value' which helps to form people's individual identity and the society in which they live. The internet was seen as affecting privacy in a way that was different to what was possible previously. The privacy as control paradigm places the individual at the centre of decision-making about personal information and which therefore may compromise the common good. While Schwartz considered that the 'data fortress' isolating personal information in an absolute sense should be avoided, he nevertheless supported limiting people from intrusion into the family lives and homes of law-abiding citizens.[701]

[693] Ibid 482.
[694] Ibid 493.
[695] Louis Lusky (1972) 'Invasion of Privacy: A Clarification of Concepts', 72 *Columbia Law Review* 693-710, 695.
[696] Ibid 696.
[697] Ibid 697.
[698] Ibid. 702
[699] Ibid 703.
[700] Paul M Schwartz, 'Internet Privacy and the State' (1999) 32 *Connecticut Law Review* 815-860, 816.
[701] Ibid, 834 and 858.

Allen supported Schwartz' view about the limitations of the 'privacy-control paradigm' in discussing its conceptual, practical and moral weaknesses.[702] She provided examples of situations in which such a paradigm would fail,[703] such as the moral accountability of personal financial disclosure for people who want access to '[w]elfare, Social Security, disaster relief, student loans',[704] and the difficulties that would be faced, for example, in health care where it is not possible to provide complete control over medical records to individuals. Allen found that 'enhancing individual control over personal data is not morally worthy as a central objective of privacy regulation' because:

> Unless people want privacy, neither government nor private sector policies aimed at individual data control and individual stewardship of personal information can insure privacy. People who ascribe to legal rights and entitlements to control personal data may choose to share more data than they conceal. They may prefer disclosure for the sake of monetary profit, artistic creation, public education medical care, commercial transaction, entertainment, or community.[705]

Lusky's attempt at a definition of privacy led him to consider that privacy should be referred to as 'the condition enjoyed by one who can control the communication of information about himself'.[706] This condition could be absolute or contingent. It would depend on the degree of control over the information. Most privacy problems were seen as fitting the contingent category and Lusky proposed five issues to be applied to each matter to assist in their resolution.[707] The aim of Lusky's analysis was to propose a rational approach to the problem of privacy rather than provide a comprehensive definition.[708]

Xu rejected 'privacy and control' and 'privacy as restricted access' in favour of the 'degree of control over information release' and the 'degree of information access by others' because he considered users apply an 'unrealistic optimism' in overestimating the control they may have

[702] Anita L Allen, 'Privacy-as Data Control: Conceptual, Practical, and Moral limits of the Paradigm' (2000) 32 Connecticut Law Review 861-875.
[703] Ibid 865-874.
[704] Ibid 872.
[705] Allen, above n 702, 871.
[706] Lusky, above n 695, 709
[707] Ibid 705: These questions are (1) Is the information literally false? (2) Is the information so incomplete as to be misleading … (3) Can procedural safeguards be devised to assure that a person who is reported upon can obtain (a) prompt notice … (b) information as to its purport, (c) an effective means of correcting any inaccuracy or material incompleteness … (4) Is the information of such a character that it can rightly be communicated only to certain persons or classes of person … (5) If and to the extent that information received from a sophisticated modern machine … is given undue weight because of the awe of that the machine inspires, how can people be made to understand that data banks know only what they are told …. ?"
[708] Ibid 710.

over information leading to an 'illusion of control'. Xu presented a multidisciplinary synthesis in the conceptual framework of the OSN domain.[709] He examined privacy literature, bounded rationality theory, control agency theory and social contract theory to analyse the issue of disclosure in OSNs, particularly the 'privacy paradox' identified in the dichotomy of privacy attitude and behaviour. In his analysis, Xu criticized the privacy control mechanism as being too narrow and excluding the aspects of privacy management beyond an individual's control.

In contrast to the view of privacy as control, the role played by context has led Nissenbaum to propose a theory of 'contextual privacy'[710] as an alternative normative theory to assist in understanding the challenges developments in technology have posed for privacy. She found conceptions of privacy such as the right to control information about oneself, the freedom from surveillance and the right to limit access as too open-ended.[711] Contextual privacy she considered the 'benchmark of privacy'[712] such that privacy is violated when either the norms of appropriateness or the norms of information distribution have been transgressed.[713] According to this theory it is:

> crucial to know the context – who is gathering the information, who is analyzing it, who is disseminating it and to whom, the nature of the information, the relationships among the various parties, and even larger institutional and social circumstances.[714]

This contextual theory is illustrated by such applications as: the movement of public records online; the consumer profiling and data mining of digital records; and the use of radio frequency identification tags. The theory is built on social analysis and the more complex social spheres of 'fields', 'domains' and 'context'[715] rather than the usual spheres of 'public' and 'private'. It is not a conceptual framework conditioned by such factors as dimensions of time or location but the right to privacy is expressed 'in terms of dichotomies - sensitive and non-sensitive, private and public, government and private'.[716] The central tenet of the theory is that 'there are no arenas of life *not* governed by *norms of information flow*' with almost everything happening 'in a context not

[709] Heng Xu, 'Reframing Privacy 2.0 in Online Social Networks' (2012) *Journal of Constitutional Law* 1077.
[710] Nissenbaum, above n 604.
[711] Ibid.
[712] Ibid 156.
[713] Ibid 139.
[714] Ibid 154.
[715] Ibid 124.
[716] Ibid 136.

only of place but of politics, convention, and cultural expectation'[717] within 'a plurality of distinct realms'.[718] Two types of 'informational norms' are proposed, 'norms of appropriateness and norms of flow or distribution' so that using contextual integrity as a benchmark for privacy, it will be violated if the informational norms have been violated.[719]

Nissenbaum does not try to 'carve a pathway through the conceptual quagmire to claim a definition" of privacy'.[720] Many authors agree that "[n]o single meme or formulation of privacy's purpose has emerged around which privacy advocacy might coalesce"[721] finding rather that privacy has a 'bad reputation' and 'an image problem'.[722]

> Every new generation of privacy scholars feels bound to navigate anew these murky waters, relentlessly citing every prior definition in an exasperating pursuit of a breakthrough. None materializes. Nor can it.[723]

Nissenbaum has been influenced by Walzer's pluralist theory of justice[724] based on a view of society as being made up of numerous distributive spheres. What matters to Nissenbaum is 'not only whether information is appropriate or inappropriate for a given context, but whether its distribution, or *flow*, respects contextual norms of information flow'.[725] In contrast to other theories of privacy, personal information is seen as tagged with a context and the 'scope of informational norms is always internal to a given context', such that what is normal is relative.[726]

The application of Nissenbaum's 'contextual integrity' theory can be seen in her analysis of the protection of privacy online.[727] The online world is not viewed as distinct but 'heterogeneous and thickly integrated with social life'. She discussed the problems created for privacy by the view of the internet as predominantly a commercial enterprise and the current failure of privacy policies or control theories involving *'transparency and choice*', questioning the assumption that

[717] Ibid 137.
[718] Ibid.
[719] Ibid 138.
[720] Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (2010) Stanford, Stanford University Press.
[721] Julie E Cohen, 'What is Privacy For' (2013) 126 *Harvard Law Review* 1904-1933.
[722] Ibid.
[723] Raymond Wacks, *Privacy and Media Freedom* (2013) Oxford University Press, Oxford, 19.
[724] Michael Walzer, *Spheres of Justice: A Defense of Pluralism*, (Basic Books, 1983)
[725] Nissenbaum, above n 720, 141.
[726] Ibid.
[727] Helen Nissenbaum, 'A Contextual Approach to Privacy Online" (2011) 140 *Daedalus, the Journal of the American Academy of Arts & Sciences* 32-48.

people understand the facts when they agree to online transactions when the privacy policies are 'long, abstruse, and legalistic'[728]. While concluding that the internet is not a 'discrete context' but rather 'the totality of experience' conducted online, Nissenbaum describes Web 2.0 as bringing 'an additional layer of changes, notably in production, creativity, and social life'.[729] Protecting privacy, whether online or offline is seen as 'a matter of assuring appropriate flows of personal information' and adopting a 'fully integrated approach' which applies 'context-based rules and expectations and embedding some of them in law and other specialized codes'. [730]

In deciding when contextual integrity should be codified into law, policy, and regulation, Nissenbaum suggested that this should occur 'when violations of norms are widespread and systematic'; when strong incentives of self-interest are behind these violations; and when 'the parties involved are of radically unequal power and wealth'.[731] As Nissenbaum has discussed, privacy as the right to control personal data with the accompanying transparency and consent has failed for reasons such as the false assumption that people can understand all the relevant facts to make a decision in relation to disclosure. There is also another underlying assumption that is problematic in that what is appropriate data flow at one time will not be appropriate at a later date. This is of significance with the permanency of data online and fails to account for changes in circumstances over time. As careers progress, past disclosures of personal data may transform into material that can damage future career development.

A further issue that has been the subject of considerable analysis is the relationship between privacy and identity. Supporting the view of privacy as a 'tool for formulating identity', Kahn[732] viewed privacy as an 'essential component of self-definition and individual development' in western liberal tradition. [733] He did not consider it should be conceptualised as merely a way of protecting property but as a 'social mechanism' to protect the individual from intrusion. Kahn did not consider it worthwhile to arrive at an authoritative definition of privacy, more important was the recognition of the role privacy plays in protecting the individual particularly from the 'debasing commodification by market forces'.[734]

[728] Nissenbaum, above n 604, 140
[729] Nissenbaum, above n 720, 38.
[730] Ibid 45.
[731] Nissenbaum, above n 604, 157.
[732] Jonathan Kahn, 'Privacy as a Legal Principle of Identity Maintenance' (2002-2003) 33 *Seton Hall Law Review* 371.
[733] Ibid.
[734] Ibid 410.

The complexity of personal identities made possible by online participation, including transactional identities has raised further challenges for privacy. Identity[735] is managed 'one application at a time' on the internet as users maintain digital identities with multiple usernames and passwords for different websites.[736] Participation in the digital pathway to justice requires a transactional identity. The question is whether this can be isolated from other forms of online identity or is there only one identity?

This has important implications for privacy on the internet, particularly as Pfitzmann and Hansen have concluded there is no such thing as 'the identity', but several of them. Identity is 'any subset of attribute values of an individual person which sufficiently identifies this individual person within any set of persons'.[737] A partial identity may be made up of particular attributes such as names or digital pseudonyms.[738] Digital identities are used in a variety of contexts, for blogs, social networks or for online transactions such as banking and efiling. The legal issues relating to the provision of digital identities by social networking sites have been explored by Tene. The issue that these authors have not explored, other than referring to the privacy problems, is to what extent each identity is entitled to privacy. Should there be degrees of privacy with a social media identity only entitled to privacy if all the privacy settings have been activated? Should a transactional identity be entitled to the highest degree of privacy?

Uniform aggregated online identities provide uniform identification for a user across many websites and together with real name policies of OSNs, interactions become less anonymous.[739] Offline, it is alleged that individuals do not have to present the same identity and have reasonable freedom to develop a 'work' and 'home' identity. Online the identity is 'tagged, categorized and stored', leading to what Nissenbaum refers to as 'fractures in contextual integrity', when identities such as those from 'work' and 'home' meet out of context. OSNs encourage data portability, particularly online identity using uniform authentication standards, to be used on sites such as Facebook and Twitter.[740] The danger lying in 'multi-directional data

[735] Andreas Pfitzmann and Marit Hansen, 'A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management', 30-31 <http://ssrn.com>

[736] Omer Tene, 'Me, Myself and I: Aggregated and Disaggregated Identities on Social Networking Services' (2013) 8 *Journal of International Commercial Law and Technology* 118-133.

[737] Pfitzmann and Hansen, above n 735, 30.

[738] Ibid 31.

[739] Omar Tene, 'Privacy: The new generations' 1 *International Data Privacy Law*, 15-27.

[740] Ibid 5.

flows' and notifications to third parties. This is in direct conflict with privacy protection.[741] Tene proposes the use of disaggregation as a solution for users with pseudonymous identities. By using pseudonyms users can gain the benefit from 'reputational capital' and also avoid their identity being aggregated under their real name. [742] The problem they face is the explicit ban on pseudonyms and disaggregation by OSNs.[743]. The wealth of personal information freely provided to OSNs is a valuable commodity.

Floridi found personal identity as 'the weakest link and most delicate element'[744] in an analysis of informational privacy. He argued that a person or agent:

> "owns" his or her information … in the precise sense in which an agent *is* her or his information. "My" in "my information" is not the same "my" as in "my car" but rather the same "my" as in "my body" or "my feelings": it expresses a sense of constitutive *belonging*, not of external *ownership*.[745]

The acknowledgment that personal information is a constitutive part of someone's personal identity and should be protected, led Floridi to conclude that this also means 'allowing that person the freedom to change, ontologically.'[746] This freedom to change will be of greater significance in the future as the generation that has developed within the digital era and is impacted by disclosure of personal information needs flexibility to redefine their identity in later life. Identity, context and control have been identified as essential elements of privacy. The issue remains whether it is possible for privacy to exist in an environment of disclosure which is in conflict with the protection of personal information.

I will examine the philosophical and public policy basis for privacy laws arguing that there is still a place for privacy in the digital world.

[741] Dan Solove, 'A Taxonomy of Privacy' 154 *University of Pennsylvania Law Review* 477, 515 where he refers to anonymity and pseudonymity protecting people from bias based on their identities and providing them with the freedom to associate and speak freely.
[742] Tene, above n 736, 125.
[743] Ibid.
[744] Floridi, above n 561, 198.
[745] Ibid 195.
[746] Ibid 197.

3.4 Philosophical and public policy basis for privacy laws

3.4.1 A place for privacy online?

While many argue that privacy is no longer possible online[747], privacy remains an important value. A review of attitudes to privacy have revealed that not only do users 'value privacy, but that the current state of privacy online represents an area of significant anxiety' and these attitudes to privacy have remained fairly constant over the past twenty years.[748] OSNs, with their demands for self-disclosure, have highlighted the extent of the privacy challenge, particularly whether it can exist at all in the current technological environment.

The privacy spikes which have followed high-profile scandals have been interpreted by Zittrain as momentary concerns, because, he considered that while polls may indicate that the public are worried about privacy, the routine disclosure of private information indicates that the concern is ephemeral.[749] This view can be contrasted with other research which has indicated that people remain concerned about the disclosure of personal information.[750] High profile cases of privacy intrusion have also created immediate concern and public reaction about privacy intrusion. They have led subsequently to government commissions and investigations. The News of the World phone hacking scandal led to public concerns about the invasion of privacy and in response, government inquiries were set up to examine the role of the media: the Leveson Inquiry in the UK[751] and the Independent Media Inquiry in Australia.[752] There was considerable

[747] David Brin, "The Transparent Society" (1998) and Neal Stephenson, "The Diamond Age" (1995); Scott McNally, CEO of Sun Microsystems at a product launch in 1999 commented on privacy, "You have zero privacy. Get over it."

[748] Timothy Libert, 'Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on One Million Websites" (2015) 9 *International Journal of Communication* 3544-3561, 3547-2548.

[749] Jonathan Zittrain, 'Privacy 2.0' (2008) 65 *University of Chicago Legal Forum* 65-119, 68.

[750] *The Economist*, 'Privacy 2.0 – Give a little, take a little', (28 January 2010) reported that research published in 2009 by the Pew Institute showed that some 60% of adults restrict access to their online profiles and in an earlier study many teenagers and young people are using privacy controls to restrict access. This article also reported that social networking sites, while having a "plethora of controls" often bury privacy statements fearing that worrying people about privacy will make them less inclined to share their personal information. Advertising and the sharing of information with application developers has become a sensitive issue. The use of mobile phones in the future, particularly for access to social networking will be a further threat to privacy. More recently the OAIC report indicated that in 2017 the majority of Australians claim to be more concerned about the privacy of their personal information when using the internet than five years ago and more than eight in ten people believe the privacy risks are greater when dealing with an organization online compared with other means: Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey 2017* (May 2017) i.

[751] Lord Leveson, United Kingdom Parliament, *An Inquiry into the Culture, Practices and Ethics of the Press* (The Leveson Inquiry), November 2012 <http://www.levesoninquiry.org.uk>.

[752] R Finkelstein QC, *Report of the Independent Inquiry into the Media and Media Regulation*, (28 February 2012) <http://www.apo.org.au/node/28522> , report to the Minister for Broadband, Communications and the Digital Economy. In this report some of the high profile cases identified included: the media coverage of the 2009 Victorian bushfires; the collar bomb case where a bomb was placed on Madeliene Pulver in August 2011; and the fire on 19 November 2011 at a Quakers Hill nursing home in Sydney. Reference was also made to the Australian Law Reform Commission report in 2008 (*For Your Information: Australian Privacy Law and Practice,* Report No 108

disapproval of media infringements of individual privacy and recommendations for the improvement of the self-regulatory system to safeguard privacy and yet allow freedom of expression.

The anxiety over online privacy has been heightened in reports detailing surveillance activities, leaks of user data and the failure of privacy protection mechanisms. Libert reported that a quantitative analysis of privacy compromising mechanisms on one million websites revealed that 'nearly nine in ten websites leak user data to parties of which the user is likely unaware'.[753] He also found that the US National Security Agency (NSA) documents leaked by Snowden revealed that one in five websites 'are potentially vulnerable to known NSA spying techniques'.[754] Libert concluded that the 'current privacy protections are wholly inadequate in light of the scale and scope of the problem'.[755]

The impact of the commercial value of personal data on privacy has given substance to the issue of whether privacy can co-exist in the online world. Researchers have attempted to estimate the value of online privacy. Acquisti and Loewenstein questioned the value of personal information and examined 'individuals' abilities to optimally navigate issues of privacy'.[756] These authors challenged the premise that it is possible to estimate precisely what privacy is worth. They found that context is important for individuals in an assessment of whether privacy is valued. In their field experiment the participants were asked to choose between gift cards with varying privacy features and monetary values. They found that dramatically different values were assigned to privacy of their personal information depending on the choice offered, for example the people who were 'willing to reject cash offers for their data was both significant in absolute terms and much larger in relative terms when they felt that their data would be, by default, protected.'[757] Their research also showed that individuals made inconsistent 'privacy-relevant' choices[758] and to avoid revealing personal information they should 'seek, install, and learn to use alternative tools

(2008) vol 2, 1472 [42.128]) which noted concern for certain information, particularly relating to children, sensitive personal health data and information relating to legal proceedings.

[753] Timothy Libert, 'Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on 1 Million Websites' (2015) 9 *International Journal of Communication* 3544-3561, 3545.

[754] Ibid. The Editorial, *The New York Times* (1 January 2014) 'Edward Snowden, Whistle-Blower' outlined the extent of the mass collection of phone and internet data and surveillance activities by the NSA <https://www.nytimes.com/2014/01/02/opinion/edward-snowden-whistle-blower.html?_r=0>.

[755] Libert, bove n 740, 3558.

[756] Alessandro Acquisti, Leslie K John and George Loewenstein, 'What Is Privacy Worth?' (2013) 42 *The Journal of Legal Studies* 249- 274.

[757] Ibid 267.

[758] Ibid 268.

[such as Tor[759]] albeit sometimes at a cost …' because often they are using default setting, particularly on social networking sites such as Facebook.[760]

As government services are increasingly being provided online, including access to legal documents, virtual courts and electronic filing, more personal data is being added to the exponentially increasing volume of information available.[761] Of concern is whether this personal data can be protected at all. It is possible, as Lessig[762] has advocated, that it may be necessary to use four mixed modalities to provide privacy protection – norms, markets, law and code. Lessig considered that code has changed the control people have over their personal data, however, it could be used to restore the traditional balance.[763] He identified two distinct problems technologies have created for privacy: increased searchability and monitoring. The solutions proposed were that searches should be minimal or justified. Code could be designed so that data was accessible without invasion. Control over monitoring was seen as more difficult. He advocated a property right in privacy which would be supported by code of a 'machine-to-machine protocol for negotiation privacy protection'.[764] What Lessig found distinctive about privacy was that individuals should be able to control their personal data with limits, such as the data people should not be able to hide or claims that shouldn't be made, avoiding sanctions for fraudulent activities or harm to others.

Froomkin has argued that information privacy could become obsolete because of the use of 'privacy-destroying technologies by governments and businesses', although technological change had not yet made legal solutions to privacy protection irrelevant. He recommended a multifaceted legal and social response would be required to provide data privacy protection before technological change became so advanced that it would be too late to provide protection.[765] In contrast, Bennett has suggested that privacy protection is an issue for

[759] Tor routes internet traffic via a network of volunteer servers using data encrypted in layers. It has been useful for dissident movements in Iran and Egypt and has also assisted access to the Silk Road international drug sale site, as reported by Dr Monica Barratt <http://monicabarratt.net>.
[760] Ibid 269.
[761] While it is difficult to estimate exactly the amount of data on the internet there are various estimates, including one estimate for 2014 is 1 yottabyte or 1.12589991 × 10^15 gigabytes.
[762] Lessig above n 83, 223. Lessig advocates consideration of four modalities for regulations: law, norms, markets and architecture or code (using technology such as Privacy Enhancing Technologies to protect privacy).
[763] Ibid, 142.
[764] Ibid 160.
[765] Froomkin, above n 570, 1461.

regulatory policy rather than as a matter to be resolved between individuals by tort claims.[766] However, the diversity of regulatory options appears to be almost as disparate as the scope of privacy itself.

For Simitis, modern data collection methods have changed the privacy debates and the protection of privacy has become 'necessary to secure the individual's ability to communicate and participate' in a democratic society.[767] Simitis considered that privacy concerned everyone, particularly as surveillance has become 'routine practice' and 'informatization … primarily a political and social challenge'. He identified four essential elements of efficient processing regulation which would create '[an] allocation of information that secures the necessary degree of proliferation without invading privacy'. These elements include recognition of the 'unique nature of personal data'; specification of the purpose for which the data will be used; continual updating and review of the regulations as well as the enforcement of data regulations by an independent authority.[768]

Once it is recognised that that privacy should be protected online, it remains an extremely difficult philosophical and regulatory issue to provide privacy protection due to the plurality of ethical beliefs in society and the contrasting bases for privacy policy.

3.4.2 Plurality of ethical beliefs

One of the fundamental problems in determining a philosophical and public policy basis for privacy laws is associated with the difficulty of identifying 'universally shared value systems in the national as well as the global context'.[769] Brownsword and Goodwin[770] recognized the dilemma for regulators in accommodating all beliefs in modern pluralistic societies. They identified the main normative frameworks relevant to technological regulation in western society as 'utilitarianism[771] (goal oriented), deontology[772] (duty based) and liberalism (rights based)',[773]

[766] Colin J Bennett, 'Privacy Advocacy from the Inside and the Outside: Implications for the Politics of Personal Data Protection in Networked Societies' (2011) 13(2) *Journal of Comparative Policy Analysis* 125.
[767] Ibid 746.
[768] Spiros Smitis, 'Reviewing Privacy in an Information Society' 135 *University of Pennsylvania Law Review* 707, 737-746.
[769] Peer Zumbansen, 'The Ins and Outs of Transnational Private Regulatory Governance: Legitimacy, Accountability, Effectiveness and a New Concept of "Context"' (2012) 13 *German Law Journal* 1269, 1277.
[770] Brownsword and Goodwin, above n 64, 51.
[771] This view has its origins in the 17th century writings of authors such as Jeremy Bentham and John Stuart Mill.
[772] Immanuel Kant, the 18th century German philosopher has been recognized as the most influential proponent of this philosophy. The deontological approach to privacy can be found in the work of Charels Fried, Stanley Benn and Jeffrey Reiman.

although they noted that other moral frameworks such as communitarianism, may be relevant. In essence the main contrasting views relevant to privacy are the view that morality of human actions is based on consequences of actions, or consequentialism, where there needs to be a balancing assessment between costs and benefits, and the view, grounded on religious or secular humanist beliefs that the morality lies in the act itself, so that invasion of privacy would be wrong innately not because of the consequences of such an action.

Lindsay argues that the values supporting privacy protection are based on 'contested views concerning human nature and the nature of society', finding that the "distinction between deontological and consequentialist approaches is of fundamental importance in evaluating claims for the legal protection of privacy".[774] The deontological view supports policies based on the protection of fundamental rights. The consequentialist view supports policies based on promoting desirable results. The choice in developing privacy law have been shown to be between a 'consequentialist or market-based approach, and a deontological or rights-based approach'.[775] This can be illustrated by the approaches to privacy law found in the US and the EU. The approach in the US was seen as more consequentialist, placing laws second to market processes. In Europe, however, the approach has been more 'Kantian-deontological', protecting autonomy and dignity from 'perceived threats of unconstrained market processes'.[776]

Lindsay proposes a 'new Foucault-influenced approach in which "privacy" should be understood in the context of ubiquitous micro-struggles over identity within totalizing social practices'.[777] His view was that privacy 'belongs at the very centre of social and political struggles in contemporary, pluralistic societies' and is a continual process of negotiating limits of individual identities found in consequentialist and deontological approaches, particularly the rights-based deontological approach.[778] He concluded that in Australia which is a 'largely consequentialist society' that a rights-bases legal approach to privacy would promote more pluralistic approaches to identity and a more effective mechanism for 'resisting global normalization and homogenization'.

[773] Brownsword and Goodwin, above n 64, 184-187.
[774] David Lindsay, 'An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law' (2005) 29 *Melbourne University Law Review* 131-178, 144.
[775] Ibid 176.
[776] Ibid 177.
[777] Ibid 134.
[778] Ibid 178.

3.4.3 A reductionist view of privacy

A direct confrontation can be found between reductionist and coherentist views on privacy. While both recognize that privacy should be protected, reductionist argue that it is not a distinctive concept and is reducible to other, more fundamental concepts such as property rights. Coherentists view privacy as a distinctive right.

Thomson,[779] in advocating a reductionist view, considered that there is such diversity and incoherence in privacy claims that they should be reduced to other more fundamental rights, such as property, confidentiality or rights to physical and personal integrity.[780] This approach was considered of limited assistance in understanding privacy by Lindsay because it strains 'our understanding of the term 'privacy' while ignoring 'the most distinctive features of the social, political and legal discourses concerning privacy'.[781]

Posner,[782] based his reductionist theory on 'an economic analysis of the dissemination and withholding of information primarily in personal rather than business contexts'. He viewed the noneconomic theories of privacy, such as the analysis by Warren and Brandeis as 'unsatisfactory'[783] and the theories of Bloustein[784] and Fried[785] as 'ethnocentric'[786]. Posner's philosophical basis for privacy policy is utilitarian and he concluded that the promise of increased understanding of privacy issues is to be found in the economic approach.

Both Thomson and Posner were writing before the digital Web 2.0 era. More recent support for reductionism can be found in the writings of Peikoff who recommended phasing out the legal right to privacy and returning to rights based on liberty, property and contract. Her thesis is that there is a guiding principle in a capitalist society of 'voluntary trade towards mutual advantage'. Therefore she considered that anyone who 'wishes to enter or remain in society and improve his standard of living by trading with others should reasonably expect, in exchange, to

[779] Judith Jarvis Thomson, 'The Right to Privacy, (1975) 4 *Philosophical and Public Affairs* 295-314.
[780] Ibid 295.
[781] Lindsay, above n 774, 145.
[782] Richard A Posner, 'The Right to Privacy' (1978) 12 *Georgia Law Review* 393-422.
[783] Ibid 406.
[784] Edward Bloustein, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39 *New York University Law Review* 962, 1003.
[785] Posner, above n 782, 407-408.
[786] Ibid 408.

give up some control over information about him'.[787]

Gavison criticised the reductionist view that 'privacy rhetoric, is misleading', concluding instead that privacy is 'useful', 'distinct and coherent'.[788] She also rejected Bloustein's suggestion that 'the coherence of privacy lies in the fact that all invasions are violations of human dignity', considering instead that dignity can be offended in ways unrelated to privacy.[789] Her support for privacy as a right related to the functions of privacy, such as 'the promotion of liberty, autonomy, selfhood, and human relations, and furthering the existence of a free society'.[790] Technological change was seen as one of the main reasons that past legal protection has become inadequate and why there was a need for an explicit commitment to privacy, although not supporting absolute protection.[791] Gavison considered that privacy in the digital era could be challenged 'in more serious and more permanent ways than ever before'.[792] She rejected both the reductionist view and the description of privacy as a form of control.

The main weakness of the reductionist interpretation has been seen as failing to acknowledge the radical change brought about by digital technologies and therefore has been found to be more suited to 'an industrial culture of material goods and of manufacturing/trading relations'.[793] It has also been seen as too easily 'overridden when other concerns and priorities, including business needs, public safety and national security, become more pressing'.[794]

3.4.4 – Privacy as property or human dignity?

The justification for privacy laws in the US has also been linked to property, often expressed as 'liberty' or the right to make personal decision without government interference. However, in the digital era the value of personal information has taken on a new dimension. It has been recognised as 'an important currency in the new millennium'[795] and a valuable commodity.[796] Littman refers to the type of personal information disclosed which is useful to commercial

[787] Amy L Peikoff, 'Beyond Reductionsim: Reconsidering the Right to Privacy' (2008) 3 *New York University Journal of Law & Liberty* 1-47, 19.
[788] Ruth Gavison, 'Privacy and the Limits of Law' (1980) 89 *The Yale Law Journal* 421-471, 422
[789] Ibid 438.
[790] Ibid 423.
[791] Ibid 467.
[792] Ibid 469.
[793] Floridi, above n 561, 193-194.
[794] Ibid 194.
[795] Paul M Schwartz, 'Property, Privacy, and Personal Data' (2004) 117 *Harvard Law Review* 2055-, 2056. Schwartz has described how companies have viewed personal data "as a corporate asset and have invested heavily in software that facilitates the collection of consumer information".
[796] Ibid 2125.

interests:

> The information that *you* (insert name, address, age, income, and social security number here) read both *Newsweek* and your daily horoscope; buy Haagen-Dazs ice cream; travel annually to New Mexico have a standing prescription for Prozac and buy a variety of different OTC antacids as well as a number of different brands of lubricated condoms; have joined three different health clubs for short sojourns over the past two years; always order a salad in restaurants; never joined Weight Watchers (and, in fact, have a 31" waist and a body mass index of 25); and give money to public television, is exceedingly valuable for the crassest of reasons: Anyone who has that information can sell it.[797]

This widespread commercialisation of the internet since the 1990s has led to a growing market in personal information, particularly as almost every online action generates 'transactional information'.[798] This information is used to market products and with this data the right to privacy has been transformed into a commodity.[799] This has had considerable impact on privacy laws in the US.

The rejection of privacy as property, with the commodification of personal data and instead a recourse to privacy as personal dignity with accompanying inalienability as found in the EU is more relevant for the digital era. This has the potential to change the focus from prevention, with the inevitable limitations, to outcomes and rectification following application to the courts.

Prins[800] asks the question, 'Would a property rights approach matter?' when such personal information becomes a commodity. The article concluded that what is important is the effect privacy as property would have on the 'limitation of misuse of personal data, and efficiency of re-use of data, especially compared to conventional human rights systems of protection privacy such as data protection law'. The reality may be that 'in the digitized trans-national world of the Internet' some property rights systems may offer more protection.[801] Prins disagreed with the view that a property rights view of privacy is in conflict with the European 'rights-based approach' because the 'European data protection system is more receptive towards a property approach than the American system' due to the 'certain instruments of control and power' over

[797] Jessica Litman, 'Information Privacy/Information Property' (1999-2000) 52 *Stanford Law Review* 1283-1313, 1285.
[798] Ibid 1283.
[799] Simon G Davies, 'Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity', in *Technology and Privacy: The New Landscape* Philip E Agre and Marc Rotenberg (eds) (MIT Press, 1997).
[800] Corien Prins, 'When personal data, behavior and virtual identities become a commodity: Would a property rights approach matter?', 3(4) *SCRIPT-ed* 270-303, 270 < https://script-ed.org/wp-content/uploads/2016/07/3-4-Prins.pdf>.
[801] Ibid.

personal information provided by the European Directive on personal property. [802]

The right to property and bodily security or an 'ownership-based interpretation' of privacy has been assessed as being problematic because of issues such as 'passive privacy' breaches where 'no informational ownership seems to be violated; in situations where informational privacy is exercised in public spaces; and non-rivalrous or 'lossless acquisition' in contrast to ownership of other property.[803]

In contrast, human dignity has been referred to as a fundamental concept that provides the framework to interpret informational privacy and 'more generally European culture and jurisdiction'.[804] It is found in Article 88 of the GDPR.[805] Floridi asserts that privacy protection 'should be based directly on the protection of human dignity, not indirectly, through other rights such as that to property or to freedom of expression'.[806] He acknowledged that there are different views of human dignity depending on what position is adopted with respect to philosophical anthropology, however, these are based on human exceptionalism and it is this philosophical understanding of human nature that will inform our knowledge of human nature in 'the digital age and our information societies'. Floridi rejected '[a]ny technology or policy that tends to fix and mould' openness because it dehumanises, rather than allowing us to 'keep our identities and our choices open'. He linked privacy to identity just as Hildebrandt has done in asserting that 'the right to privacy is "the freedom from unreasonable constraints on the building of one's identity"'.[807]

Informational privacy in Europe is concerned with the application of privacy to personal information, referred to as data protection. The principles are outlined in the EU Data Protection Directive which incorporated Article 8 of the *European Convention on Human Rights*

[802] Ibid 302.
[803] Floridi, above n 561.
[804] Floridi, above n 667.
[805] Article 88 – Processing in the context of employment … 2. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a groups of enterprises engaged in a joint economic activity and monitoring systems at the work place.' The GDPR was approved by the European Parliament on 14 April 2016.
[806] Floridi, above n 548.
[807] Mireille Hildebrandt, 'Location Data, Purpose Binding and Contextual Integrity: What's the Message?', Chapter 3 in L Floridi (ed) *Protection of Information and the Right to Privacy – A New Equilibrium?* (Springer International Publishing, 2014) 31-62, 57.

(ECHR). The application of Article 8 was demonstrated in *Von Hannover v Germany*[808]. The Court recognized that protection involves more than the private family and extends to anyone, even if they are well known so that they are able to 'enjoy a 'legitimate expectation' of protection of and respect for their private life'. This was considered fundamental to 'the development of every human being's personality'.[809]

The concept of privacy as 'deriving from human dignity' has been supported by Eltis, whose concern is that privacy should be a 'facilitator' not a 'detractor of accessibility', particularly in the context of its impact on the judiciary and the courts.[810] Eltis has suggested reframing the debate in the context of the internet with a broader understanding of privacy so that it can be viewed as a 'facilitator rather than a detractor of accessibility', particularly in the context of its impact on the judiciary and the courts.[811] Instead of viewing access and privacy as conflicting concepts, she considered that they could be complementary. A large part of the apparent conflict being the principle of open courts and the perception that in preserving open courts in the digital era, privacy would be compromised and people discouraged from participating in the justice system where they would be faced with 'humiliation, intimidation and retribution' through the release of private information. Eltis argued that this approach would enable judges to use their discretion to protect litigant's privacy without undue concern that the principle of open courts was sacrificed

Eltis concluded that privacy is an affirmative rather than negative right,[812] a right to 'engage in individual self-definition and self-invention' and the 'responsibility not to unnecessarily compromise one's own information'. The 'reasonable expectation' standard of the Anglo-American conception of privacy is viewed as not responding to the impact of technology which

[808] *Von Hannover v Germany* [2004] ECHR 294 (24 June 2004). Princess Caroline of Monaco complained about photographs taken without her permission which were published in a variety of German magazines. The court held that the photographs were protected by Article 8 and found that this Article protected individuals against arbitrary interference by public authorities and protection for private life in the relationships between individuals. The photographs did not contribute to a debate of general interest. A later application by Princes Caroline in *Von Hannover (No 2)* in 2012 where the photograph showed her and her husband on a skiing holiday in St Moritz together with an article about the ill health of Prince Rainer III where held not to have infringed Article 8 and Article 10 because it contributed to a debate of general interest. A further application and decision handed down in September 2013 the European Court held that the German Federal Court's refusal to grant an injunction to prohibit further publication of a photograph and article about the vo Hannover family villa on an island in Kenya did not breach Article 8 because the article gave few details about their private life.

[809] *Von Hannover v Germany* [2004] ECHR 294 (24 June 2004) [69].

[810] Eltis above n 413, 316.

[811] Ibid.

[812] Karen Eltis, 'Breaking Through the "Tower of Babel": A "Right to be Forgotten" and How Trans-Systemic Thinking Can Help re-Conceptualize Privacy Harm in the Age of Analytics' (2012) 22 *Fordham Intellectual Property, Media & Entertainment Law Journal* 69-95, 95.

will limit 'spatial seclusion'.[813] Eltis contrasts the protections in the off-line world with the internet of 'infinite memory'.[814] As the legal change cannot keep pace with technological innovation, the solution proposed by Eltis is to correct the problems after privacy intrusion has occurred so that people can 'erase' the harm.

3.4.5 Reformulating the balance: a new equilibrium

A way forward in developing a new conceptual framework, particularly in the context of law enhancing access to law using innovative technologies, is to adopt a philosophical analysis. This has been provided by authors such as Richardson, drawing on the work of Spinoza and by Floridi's ontological interpretation of informational privacy for whom communication 'is central to their conceptual frameworks in ways that are derived from their ontology'.[815] Richardson contrasts the commodification of privacy by authors such as Posner.

Floridi's ontological theory of informational privacy is based on information ethics.[816] He views accessibility 'as an epistemic factor that depends on the *ontological features* of the infosphere'. These features are held to 'determine a specific degree of *ontological friction*, which in turn determines the information flow within the system'. Therefore, he considered that the greater the friction the less information flow and lower levels of accessibility. Floridi distinguished between old technologies and new digital technologies. These he viewed as interactive and themselves '*ontologizing devices*'. Digital technologies, because they allow forms of protection, can 'both erode and reinforce informational privacy'. He considered informational privacy as extremely important because 'one's informational sphere and one's personal identity are co-referential'. Floridi contrasted the ontological interpretation with consequentialist views which can accept informational privacy being overridden. He did not agree that the protection of privacy should be based indirectly on other rights, such as property or freedom of expression. He argued that by equating the protection of privacy to personal identity' it becomes 'a fundamental and inalienable right'.

Furthermore, he considered that by changing perspective, it is no longer necessary to consider informational privacy with the 'false dichotomy' of a public or private context. Floridi compared informational privacy to 'kidnapping rather than trespassing', to illustrate that

[813] Karen Eltis, *Courts, Litigants and the Digital Age – Law, Ethics and Practice* (Irwin Law Inc, 2012).
[814] Ibid 7.
[815] Janice Richardson, *Law and the Philosophy of Privacy* (Routledge, 2016) 5.
[816] Luciano Floridi, 'Four challenges for a theory of informational privacy' (2006) 8 *Ethics and Information Technology* 109-119, 109.

kidnapping would be a crime independently of whether is occurred in public or private. Floridi agreed with Warren and Brandeis in their discussion of 'the more general right of the individual to be let alone', as one of 'inviolate personality' rather than 'the principle of private propriety'. For Floridi's the protection of informational privacy means allowing a person 'the freedom to change, ontologically'.

Floridi's theory of informational privacy has been challenged on the basis that it does not differentiate informational privacy from other kinds of privacy nor does it 'distinguish between descriptive and normative aspects of informational privacy'.[817] Tavani viewed Floridi's theory as one that could supplement existing privacy theories and provide a 'novel way of analysing the impact that digital technologies have had for informational privacy'.[818] What is unique in Floridi's analysis is the direct link that he provides between privacy and the reasons for protecting it in the digital era. As he has stated:

> privacy is to be protected because of human dignity, which is to be protected because of human exceptionalism, which is to be explained and defended by a specific philosophical anthropology, which is in its turn in need of a justification.

This major shift in analysis, Floridi found necessary in the digital era of 'endless expansion' of the personal data online.[819] Privacy is not deconstructed into bodily privacy or informational privacy but it is a unitary concept linked to identity and being. It is an analysis that make it unnecessary to qualify informational privacy as public or private because information is viewed as context independent.[820] It is an interpretation that draws together the essential issues discussed earlier of control, context and identity.

3.5 Conclusion

The necessity for a paradigm shift in the conceptualisation of 'personal information' and 'privacy' has been dictated by technological developments over the past 25 years. The transformation of technologies from a centralised, managed structure of mainframe and desktop computers to mobile platforms, interactive applications, OSNs global commercialism in networks has made the protection of personal information a formidable task. The need for continual change in regulatory response is reflected in the current replacement of the EU

[817] Herman T Tavani, 'Floridi's ontological theory of informational privacy: Some implications and challenges' (2008) 10 *Ethics and Information Technology* 155-166.
[818] Ibid, 155.
[819] Luciano Floridi, 'The Onlife Manifesto' <https://ec.europa.eu/digital-agenda/en/onlife-initiative> 12.
[820] Floridi, above n 561, 195.

Directive 95/46 with a General Data Protection regulation to ensure continued security, rights of access and rectification of data with 'supervisory authorities and access to the courts'.[821]

The initiatives of e-Government have added a more complex and acute perspective to the personal data and privacy agenda.[822] As technology has fundamentally changed the nature of transactions between governments and individuals, it has become more difficult for privacy laws to adequately protect the personal information required for such transactions".[823] As a recent report by Australia's Auditor-General[824] considered that '[u]nauthorised access and misuse of government information[825] is an international issue which can affect, amongst other things, national security, the economy, personal privacy, and the integrity of data holdings'.

Paradoxically, the benefits promised by Web 2.0 of enhanced access to justice have also created risks and regulatory challenges. Disclosure of private information has the potential to frustrate access to justice in an 'Internet of infinite memory'.[826] Participants in the digital world increasingly face the dilemma that online self-disclosure of personal information is demanded as the price of participation for access to many services, government, legal, commercial or social, personal information. Users are severely compromised by disclosure of personal information, with misuse, its aggregation, sale and deliberate or inadvertent disclosure. The commercial value of personal data, new technological means of surveillance and confusion over what is 'public' and what is 'private' in online spaces have made the formulation of legitimate, effective and connected regulations challenging.

In looking toward the future, Faris and Heacock have found that it has become increasingly difficult to protect privacy:

> from governments, companies, or other users … and state surveillance is compounding a growing uneasiness regarding the acquisition, use and

[821] Denis Kelleher, 'EU Data Protection Law: The First 25 Years' (5 November 2015) *Privacy Perspectives* <http://www.iapp.org>.
[822] N Robinson et al, "Review of the European Data Protection Directive" RAND Europe Report (May 2009) prepared for the Information Commissioner's Office UK, 13 – 15.
[823] Clare Sullivan, 'Digital Citizenship and the Right to Identity in Australia' (2013) 41 (3) *Federal Law Review* 557, 582.
[824] Auditor-General, Australian National Audit Office, 'Cyber Attacks: Securing Agencies' ICT Systems: Across Systems' (Audit Report No 50 2013-14 Performance Audit) 17<https://www.anao.gov.au/sites/g/files/net616/f/AuditReport_2013-2014_50.pdf>
[825] Ibid. The Report referred to 1790 security incidents against Australian Government agencies between January and December 2012 and in 685 of these incidents the Cyber Security Operations Centre was consulted due to the seriousness of the incidents, 12.
[826] Eltis, above n 812, 73.

> distribution of personal information by private sector companies. Moreover, the ability of the state to collect information on people is supported by private sector data collection and the willingness of users to share information in private, semi-public, and public spaces online.[827]

These concerns are aggravated by the 'cross-border flow of people, goods, services, and information that characterizes globalization' which has put 'increased pressure on national legal systems, and underscored the need for policymakers to address the costs associated with regulatory fragmentation'.[828] Tréguer has asserted that 'new institutional frameworks need to be designed to allow governments, businesses and private individual alike to work together across borders'.[829] An interconnected world is essential where interoperability is a 'critical building block' allowing legal systems to work together and demonstrated the need for a conceptual convergence, particularly a resolution to the policy confrontation between the EU and the US over international data flow.

Brownsword and Goodwin, in reviewing the 'ethical limits that communities set for themselves through the trope of boundary-marking concepts',[830] has found that the necessary indeterminancy of human rights means that they cannot overcome boundary disputes or the 'incommensurability between different ethical outlooks'. Where there is radical disagreement over the ethical boundaries, the use of public participation has been suggested as more useful for the public policy of regulating issues such as privacy.[831] The US approach to privacy and cultural bias with its emphasis on ownership and property has been viewed as avoiding the public discussion in the political arena 'where human rights are a primary concern' and where '[s]ocially constructed norms of privacy can and must evolve.[832]

The recent developments in technology have been seen as undermining privacy 'while courts and legislators have been advancing privacy interest, technology has been working to destroy

[827] Rob Faris and Rebekah Heacock, 'Looking Ahead' Internet Monitor 2013: *Reflections on the Digital World* The Berkman Center for Internet & Society at Harvard University Research Publication No 2013-27 (December 12, 2013) <http://ssrn.com>.
[828] Ibid.
[829] Félix Tréguer, 'Interoperability Case Study – The European Union as an Institutional Design for Legal Interoperability' ,The Berkman Center for Internet & Society at Harvard University Research Publication No 2013-27 (September 2012) <http://ssrn.com>.
[830] Brownsword and Goodwin, above n 64, 188.
[831] Ibid 268.
[832] Divian Fraru-Meigs, 'From Secrecy 1.0 to Privacy 2.0: Who Controls What" Critical Review Essay' (2010) 123 *Revue Francaise D'Etudes Americaines* <https://www.cairn.info/revue-francaise-d-etudes-americaines-2010-1-page-79.htm>

them'.[833] Court records have been described as sources for an aggregation of personal data, particularly as court records are moved from local to online access.[834] A study of the 'disruptive potential of electronic media and digital networks'[835] concluded that the 'courts have an obligation to rewrite rules governing the creation of, and access to, public court records in light of substantive changes that online access augurs'.[836] Participants in the legal system need to be confident that their personal information will be protected. Privacy and access to justice were viewed by Eltis as concepts in conflict but 'privacy in the electronic court records context might ultimately be *about* the very access to justice we seek to protect'.[837] She argued that the 'illusion' of access created by 'unbridled postings' needs to be regulated by court control over documents and the protection of personal data, arguing by protecting privacy access to justice becomes more available. To achieve both open justice and privacy in the digital age, the courts need to engage in a 'new and complicated exercise of line-drawing' to ensure that the open courts principle is sustainable[838] and respond to the 'increasing social and economic significance' of privacy.[839]

It is no longer a reasonable assumption, as Warren and Brandeis had made in the 1890s, that because people have disclosed information it is no longer private. The complexity of the disclosure, facilitated by developments in technology, can be seen as ranging from forced disclosure to aggregated, contractual and transactional disclosure with a resultant unintended permanency and distribution that has called for a redefining of the nature and extent of the protection required.

It is the exposure of personal information enabled by such disruptive technologies as OSNs and their impact on access to justice that I will analyse in the following chapter. OSNs are innovative technologies which provide a new paradigm of online communication, challenging the rule of law. Floridi's ontological framework will be used to both understand how they are able to enhance and challenge the protection of privacy and personal data.

[833] Beverley McLachlin, Chief Justice, 'Openness and the Rule of Law' (Paper presented at the Annual International Rule of Law Lecture, London, 8 January 2014) 13.
[834] Conley et al, above n 292.
[835] Ibid 776.
[836] Ibid 777.
[837] Eltis, above n 413, 291.
[838] McLachlin, above n 833, 25.
[839] Lindsay, above n 774, 143-144.

Chapter Four – Online social networks: enhancing or diminishing access to justice?

4.1 Introduction

Online social networks (OSNs) have the capacity to facilitate or obstruct access to justice by amplifying or constricting the flow of personal information. They are the most 'disruptive' technological development of the innovative applications of Web 2.0. They conform to a large degree to the analysis by Christensen[840] in performing differently to established methods of communication, mostly free to use, more convenient and simpler. However, their use by the legal system raises a fundamental concern for the enhancement of access to justice: how can the tension between the engagement with such innovative technologies and the rule of law be resolved?

The legal regulatory environment has been confronted by OSNs which provide a new communications paradigm of disclosure, not previously experienced before the digital era. This has transformed open access and transparency, responsive dialogue and a voice for the courts, however these features have also presented a challenge to 'fundamental aspects of the rule of law'.[841] The challenge for regulators is to establish 'acceptable risk regulation'[842] enabling the employment of new technologies while assisting access to justice.

The use of online social networks had become ubiquitous by the first decade of the 21st century.[843] The demographics of users indicated that the use of the internet for communication, particularly 'for creating, cultivating, and continuing social relationship – is undeniable'.[844] This

[840] Christensen, above n 5. See also discussion of 'disruptive technologies' in Chapter One of this thesis.

[841] Chief Justice Marilyn Warren, 'Open Justice in the Technological Age' (2013) 40 *Monash University Law Review* 45-58.

[842] Brownsword and Goodwin, above n 64, 165.

[843] PewResearchCenter, Andrew Perrin, *Social Media Usage: 2005 – 2015* (October 2015). By 2015 65% of adults in the United States were reported as using social networking sites <http://www.pewinternet.org>.

[844] A report on online usage in Australia in 2012 (ExactTarget report, #15, 'Digital Down Under' <http://www.exacttarget.com.au>) indicated that 13.4 million Australian spend an average of 18.8 hours per day online with 1 in every 5 minutes being spent on social media. Twenty seven per cent of Australians will check Facebook as the last task of the day. There are almost ten million unique visitors to Facebook each month or approximately 42 per cent of the Australian population. Twitter use is also high in Australia with 51 per cent of the active Twitter members checking the site once a day. There are just over 1 million unique visitors to Twitter each month or 4.8 per cent of the Australian population. Australians were also spending a considerable amount of time online with one in five minutes a day spent on social media. By 2015 the Sensis Social Media Report ('How Australian people and businesses are using social media' <http://www.sensis.com.au/socialmediareport>) found increased levels of engagement with online social networks, particularly as about 70% access networks from their smartphones. The overall use was noted as reaching a plateau compared to previous years. However, they have become "a critical way in which the public, business and governments are communicating" with close to 50% of consumers accessing online social networks every day. Facebook was found to be the dominant online social network with 93% of users and they spend eight and a half hours per week on this site.[844] LinkedIn and Twitter account for 28% and 17% respectively.

generalised usage of OSNs for communication and public expectations have placed pressure on courts to determine whether they can be used as an effective form of communication.

Ironically these innovative applications which promise the most open access also present the most danger to a fair trial and may undermine the integrity of the judicial system. Lord Judge, Chief Justice of England and Wales, in commenting on this disruption, particularly the Twitter posts disclosing the identity of high profile applicants for injunctions, declared that modern technology is 'out of control'.[845] It is therefore not surprising that the adoption of OSNs for communication by the courts has been cautious and a reflection of a policy of regulatory prudence[846] adopted by the courts in the face of the dynamic and disruptive nature of OSNs.

Despite only a very small number of courts using OSNs by 2010, it has been predicted that once there is reconciliation between 'the judicial and new media cultures', more courts will develop a presence on Facebook, Twitter, YouTube and other OSNs.[847] By September 2015 there was some indication of changing attitudes in Australia with Twitter being actively used by courts in New South Wales and South Australia.[848] This indicated both an objective of the courts to engage in direct communication with the public and to meet the expectations of open justice. Chief Justice Marilyn Warren explained the necessity for Australian courts to adapt to this new communication channel, while protecting the rule of law:

[845] Owen Bowcott, 'Superinjunctions: Modern technology out of control, says lord chief justice' (Friday 20 May 2011) <http://www.theguardian.com>; the Chief Judge indicate this view had been modified when he stated that such technologies could be used "provided that we are tis masters and that it is our tool and servant".

[846] Brownsword and Goodwin, above n 64, Chapters 6 and 7.

[847] Conference of Court Public Information Officers, *New Media and the Courts: The current status and A Look at the Future* (August 25, 2010) 87, ttp://www.ccpio.org> This report found at 66 that "[w]hile more than a third of the respondents agreed that courts as institutions can (1) maintain a social media profile site, or use (2) a microblogging technology or (3) visual media sharing websites without compromising ethics, just 7 percent or fewer work for a court that actually engages in such an activity". The United States Supreme Court joined Twitter in June 2009 and District Court of California in June 2009. The California Administrative Office of Courts began using the California Courts YouTube Channel and Twitter in July 2010 "to complement its ongoing public education and outreach efforts about the judicial branch of government and access to justice"[847]. The UK Supreme Court began using Twitter in October 2011 and other United States Courts were found to have joined by 2012, including the Washington Courts.[847]

[848] Alysia Blackham and George Williams, 'Courts and social media: Opportunities, challenges and impact' (November 2014) 17 *Internet Law Bulletin* 210-213. Blackham and Williams found that only a few Australian courts had adopted these applications to assist court communication, although, the Family Court of Australia had opened a Twitter account in October 2012. They noted that the Federal Circuit Court had opened an account, not to use immediately, but to ensure it had the preferred Twitter name if it later decided to use it later and the Federal Court had closed its inactive Twitter handle[848]. By September 2015 there was some indication of changing attitudes and more courts were found to be actively using Twitter, including the New South Wales and South Australian courts[848] to aid communication and make court processes more accessible.

> There is an expectation that open justice involves the judiciary adopting new media technologies and engaging in a direct dialogue with the community. The judiciary must find a way to meet these expectations whilst at the same time preserve the fundamental aspects of the rule of law – fairness and judicial impartiality.[849]

Her Honour considered that courts must develop constructive communication strategies to engage with the internet and social media because '[o]pen justice in the technological age means the ability of the community to view or access information about court proceedings through the internet or social media as well as through traditional print and electronic mediums".[850] The communication strategies adopted by the Supreme Court of Victoria, which will be analysed in more detail later in this chapter, recognises the changing relationship between courts and the public.

The nature of engagement between the courts and the public has changed in the era of OSNs.[851] It has been found that 'courts have become increasingly visible, first via Web 1.0 … and, more recently, by Web 2.0'.[852] The 'changing interface between the courts and the media' were argued to be 'irrefutable'[853] especially as courts have 'had Facebook, Twitter, YouTube and blogs thrust upon them'.[854] However, the dilemma for courts was seen by Schulz and Cannon[855] to be to engage with social media while maintaining the integrity and independence of the judiciary. The implications of social media emergence was viewed as making a major impact on discourse in modern society, a discourse courts could not ignore. In a more detailed analysis of the role of communication in providing access to information about the courts, Schultz[856] highlighted the dangers of ignoring effective communication in the face of 'the discourses of *disapproval, disrespect, debate, diminution* and *direction'* [857] and general anti-justice discourse confronting the courts. The choice faced by the courts is whether they should remain 'separate, independent

[849] Warren, above n 841, 58.
[850] Ibid 15.
[851] Patrick Keyzer, 'Who Should Speak for the Courts and How? The Courts and the Media Today in Patrick Keyzer, Jane Johnston and Mark Pearson (eds) *The Courts and the Media: Challenges in the Era of Digital and Social Media'* (Halstead Press, 2012).
[852] Jane Johnston, 'Courts' New Visibility 2.0' in *The Courts and the Media: Challenges in the Era of Digital and Social Media'* Patrick Keyzer, Jane Johnston and Mark Pearson (eds) (2007) Halstead Press, ACT 41. Johnston refers to Web 1.0 as 'predominantly websites' and Web 2.0 as 'predominantly social media'.
[853] Ibid 42.
[854] Ibid.
[855] Pamela D Schulz and Andrew J Cannon, 'Trial by Tweet? Findings on Facebook? Social Media Innovation or Degradation? The Future and Challenge of Change for Courts, (February 2013) *International Journal for Court Administration* 1-9.
[856] Pamela D Schulz, *Courts and Judges on Trial – Analysing and Managing the Discourses of Disapproval* (Transaction Publishers, 2010).
[857] Ibid 101.

and above the fray', leaving them 'misrepresented, diminished and ultimately irrelevant'[858] or whether they should engage with OSNs. The maintenance of their own communications strategy has been regarded as essential to maintain the rule of law by ensuring that the community is accurately informed.[859]

Certain characteristics of OSNs make them valuable channels for direct communication, particularly the instantaneous nature of the applications and their facilitation of expression by the use of links to articles and audio-visual materials. The combination of the extraordinary growth in OSNs with the increase in civil litigation of the numbers of self-represented litigants has been predicted by Robertson[860] to transform 'traditional legal practice' and expand access to justice from the bottom up by 'constituents who have not traditionally been participants in the legal market' who are able to use social networking tools.[861] This contrasts with the disruptive theory of Susskind which, according to Robertson, focuses on the impact of technological change at 'a fairly high-end side of the legal market'.[862] She agrees with Susskind's prediction that 'a new interface will emerge between the non-lawyer and the law, between the citizen and the State'.[863] Previously, the legal profession has been the interface because the law was too complex for individuals to manage their cases, however with the development of technology legal services have become faster, cheaper and more available[864] and it will be possible for more people to pursue their claims due to the 'information, connectivity, and communication'[865] provided by social media, particularly to self-represented litigants.

Susskind's reservation, however, was that genuine access to justice would not be achieved unless there is effective promulgation and a second generation of legal information made available to assist people to recognise 'if and when they need legal guidance' and to assist them to know when laws have been changed.[866] He recognised that the development of Web 2.0 methods of communication, such as blogs and various forms of discussion forums people could be

[858] Schulz and Cannon, above n 855, 3.
[859] Ibid.
[860] Cassandra Burke Robertson, 'The Facebook Disruption: How Social Media May Transforms Civil Litigation and Facilitate Access to Justice' (2012) 65 *Arkansas Law Review* 75-97.
[861] Ibid 3.
[862] Ibid.
[863] Susskind, above n 55, 283.
[864] Ibid 284.
[865] Robertson, above n 860, 26.
[866] Susskind, above n 55, 262.

'informed in a digestible way' about new laws.[867] Lord Neuberger recognized that in principle tweeting would be 'an excellent way to inform and engage interested member of the public, as well as the legal profession' and an activity that should be accepted unless it interfered with the hearing.[868] Not all judges have approved of the use of OSNs, considering them to be an inappropriate method of communication, particularly for the courts.[869]

The increasing use of Web 2.0 collaboration has been described as a 'tectonic shift for the legal profession' with the immense power of networked collaboration provided by social networks such as Facebook.[870] Their use by the legal profession was viewed in 2008 as being driven by the scale and complexity of legal work and the need for 'multi-jurisdictional information' with these new technologies allowing 'users to be autonomous and collaborative, simultaneously'.[871] By the first decade of the 21st century they had become a global phenomenon.[872] They have created 'unprecedented opportunities for the courts to engage with journalists and the wider community'[873] but at the same time posed 'intense challenges for the law and judicial administration'.[874]

This chapter will analyse the different characteristics of OSNs and examine the opportunities and challenges they present for the courts. These features, particularly the opportunities for enhancing access to justice, will be assessed by an in-depth analysis of the use of Twitter by the Supreme Court of Victoria.

[867] Ibid 264.

[868] Lord Neuberger, above n 423, 269.

[869] Judge J C Gibson, 'Judges, Cyberspace and Social Media', (2014) based on a paper presented for the Australasian Institute of Judicial Administration annual conference, July 2013 and a paper 'Judicial Style and Reasoning' for the 2009 China Law Society, <http://www.aija.org.au>; Gibson J refers to the decision of Ouseley J in not permitting Twitter to be used in reporting *Swedish Authorities v Assange* [2010] EWHC 3473 (Admin). His Honour considered [3] that there was a "potential for distraction and disruption to the appropriate atmosphere of the court".

[870] *Fortunato v Chase Bank USA* 2012 *U.S. Dist. LEXIS 80594*. In this case Judge Keenan decided that Chase had not produced facts to prove that the Facebook profile was maintained by the plaintiff's daughter and commented that anyone could make a Facebook profile using real, fake or incomplete information.

[871] Ibid 41.

[872] danah m boyd and Nicole B Ellison, 'Social Network Sites: Definition, History, and Scholarship' (2008) 13 *Journal of Computer-Mediated Communication* 210-230, 217-219.

[873] Patrick Keyzer et al, 'The courts and social media: what do judges and court workers think?" (2013) 25(6) *Judicial Officers' Bulletin* 47-51.

[874] Ibid 47.

4.2 The nature of online social networks

OSNs are available to most people who have access to the internet and have the potential to reach many people who have not been able to access the courts, particularly the growing number of unrepresented litigants. Not all OSNs are the same. New ones emerge and the popular OSNs are constantly evolving and transforming, offering new features and replacing others. There are hundreds of differing applications and websites which can be labelled OSNs, some more popular than others. Some offer more visual content, others are more text based. These OSNs can be open networks, available to all members of the public or closed networks, available to a select group. What is significant, as Floridi has found, was that the combination of personal data and the participation in OSNs has involved the 'online construction of a personal identity' in the 'infosphere' which 'is not just a medium, but the new environment where groups and individuals continuously and increasingly define themselves'.[875] Floridi refers to comments that for those who have never experienced life in adulthood without OSNs, participation is not optional. Participation has become 'identity-constraining' because people feel the need to constantly stream photos, thoughts and other personal data to 'ensure the virtual version of you is accurate'.[876]

The platform for the evolution of online social networks is Web 2.0[877] and its 'ideological and technological foundation'[878] which has made possible the creation of online user-generated content, transforming 'static, unidirectional, mass communication tools' into 'highly interactive, dynamic and community-orientated' websites.[879] The two-way culture of communication is exemplified by online social networks that enable users to post personal data, photos, messages, audio-visual files and distribute them to a wide network of contacts. Their use has evolved rapidly with many users accessing OSNs 'every day or multiple times per day',[880] particularly on mobile devices and smartphones. [881]

[875] Luciano Floridi, 'The Construction of Personal Identities Online' (2011) 21 *Minds & Machines* 477-479, 478.
[876] Ibid.
[877] Various concepts and practices have been identified which distinguish Web 2.0 applications. These features include social software 'predicated on microcontent'[877] which is collaborative and open in contrast to Web 1.0's more static content: see discussion in Chapter One. Although the term 'Web 2.0'[877] itself has been labelled 'audacious' with features too diverse and evolving to define[877].
[878] Andreas M Kaplan and Michael Haenlein, 'Users of the world, unite! The challenges and opportunities of Social Media' 53 *Business Horizons* 59, 61.
[879] Evan E North, 'Facebook Isn't Your Space anymore: Discovery of Social Networking Websites´ (2010) 58 *Kansas Law Review* 179, 1288.
[880] Sensis, *Sensis Social Media Report 2016: How Australian businesses are using social media* (1 June 2016) 3. This report referred to the 'almost ubiquitous appeal – 95% of users' of Facebook at 4. It found that 69 percent of Australian are on social media with 57% of people accessing social media every day or most days: <https://www.sensis.com.au/about/our-reports/sensis-social-media-report>.
[881] Ibid. It was reported that 72 per cent of users accessed the applications on their smartphones.

Innovative OSNs can be referred to by the more general term, 'social media'. This has been defined as:

> Highly interactive, multimedia, websites and programs that allow individuals to form into communities and share information, knowledge and experiences more quickly and effectively than ever before.[882]

It has also been referred to as:

> A group of Internet-based applications that build on the ideological and technological foundations of [the worldwide web] which allows the creation and exchange of user-generated content.[883]

They have been identified as having characteristics:

> (a) that enables users or subscribes to create, display, and maintain a profile or Internet domain containing biographical data, personal information, photos, or other types of media,
>
> (b) that can be searched, viewed, or accessed by other users … with or without the creator's permission, consent, invitation or authorization, and
>
> (c) that may permit some form of communication, such as direct comment on the profile page, instant messaging, or email, between the creator of the profile, and users who have viewed or accessed the creator's profile.[884]

A defining feature of OSNs was found to be its 'interactive and two-way', 'participatory culture' that is easily accessible and in which the 'creator relinquishes control of the message'.[885] Boyd and Ellison[886] considered that the unique aspect of social network sites was that they have allowed users to 'articulate and make visible their social networks'.[887] They have defined social network sites as:

> Web-based services that allow individual to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a

[882] Conference of Court Public Infor. Officers, New Media Comm., *New Media and the Courts: The Current Status & a Look at the Future* (2010) <http://www.ccpio.org>.
[883] Kaplan and Haenlein, above n 878, 61.
[884] Neb. Rev. Stat. § 29-40001.01(09) (2010)
[885] ResearchGate, *Juries and Social Media, A report prepared for the Victorian Department of Justice* (2013) 2, <https://www.researchgate.net/publication/275037791>.
[886] boyd and Ellison, above n 872, 211.
[887] Ibid 11.

> connection, and (3) view and traverse their list of connections and those made by others within the system.[888]

A variety of technical features such as visible profiles, the identification of other members with whom they share a connection or relationship, a public display of these connections, mechanisms to leave messages and comments as well as mechanisms to send private messages characterise OSNs. They have also been referred to as 'new media',[889] an umbrella term characterised by developing interactive social media which are multimedia, 'decentralized and multidirectional' and 'personal and intimate'.

Some OSNs are more suitable for courts to use to establish interactive communications than others. An examination of the types of OSNs reveals considerable diversity, presenting different opportunities and risks for access to justice. While law firms around the world are engaging with online networks[890] they have been found to have been slow to utilise the communication opportunities offered. It has been considered that OSNs will form part of the way law firms communicate, gather and disseminate information in the future. LinkedIn has emerged as the 'primary non-sector-specific platform' used by law firms, although they are not using some of the advanced features of this application. Twitter has been found to be used mainly for broadcasting information with only a few law firms using the application interactively. While some law firms were creating content on social networks, most activity was discovered in English-speaking countries with blogging and social media integration in the very early stages of development. Western Europe was viewed as the leader in social media usage in the legal sector. Of the regions examined, the Asia Pacific region demonstrated the least amount of social media usage, however Sydney was viewed as an exception.[891]

Open networks are available to the general public and allow a free flow of information with limited 'ontological friction'[892] and therefore limited privacy protection. To join, an account is opened by the submission of personal information. Facebook, LinkedIn, YouTube and Twitter

[888] Ibid.
[889] The Conference of Court Public Information Officers (CCPIO) has worked in partnership with the National Center for State Courts and the E W Scripps School of Journalism at Ohio University and prepared reports since 2010 from surveys sent to judicial officers, courts' staff member or other court-related personnel, attorneys, college professors and law librarians. <http:www.ccpio.org>.
[890] Martindale-Hubble, *Global Social Media Check Up – A global audit of law firm engagement in social media methods* (2011) http://www.mrtindale-hubbell.co.uk/socialmedia>.
[891] Ibid 7.
[892] Floridi, above n 561.

are amongst the most popular OSNs[893] with the number of overall users of OSNs worldwide increasing steadily since 2010.[894] The main features of Facebook have been described in cases such as *Australian Competition and Consumer Commission v Allergy Pathway Pty Ltd and Anor. No 2.*[895] In a decision of the High Court of Justice in Northern Ireland in 2013 McCloskey J, in an application for an interim injunctive order against Facebook, discussed some of the terms and conditions of Facebook.[896] It was held that even if privacy settings were activated it was found, these settings are 'not effective to prevent a user from being "found"'.[897]

Twitter[898] was described in *Chambers v Director of Public Prosecutions*[899] as a social networking platform, invented in 2006, and owned and operated by Twitter Inc, an American corporation which is accessed on the internet by registered users. Registered users adopt a unique user name or 'Twitter handle' and are then able to post messages or 'tweets', of no more than 140 characters which are 'no more and no less than conversation without speech'.[900] Twitter users can be followed and they can converse with other Twitter users. A public time line shows the most recent tweets which remain visible for a short while and they are then replaced by more

[893] There were approximately 400 million members of LinkedIn worldwide in 2015. This had increased to approximately 470 million by 2016 <https://www.statista.com> of these users there were approximately 3.4 million in Australia in 2015 which had increased slightly to 3.6 million by February 2017 <https://www.socialmedianews.com.au>.

[894] In 2010 there were close to 1 billion users of OSNs. By 2015 this had increased to over 2 billion users and by 2017 was reported as 2.5 billion <https://www.statista.com>.

[895] *Australian Competition and Consumer Commission v Allergy Pathway Pty Ltd and Anor. No 2* (2011) 192 FCR 34 In this case Justice Finkelstein described the main access feature of Facebook and Twitter. 'Only those people who the user has accepted as a friend can post on the user's wall. A user is able to delete messages posted by friends on the user's wall. A Facebook user can choose who can see particular parts of his/her Facebook page … While a user must confirm a person to be their friend, a user elects to become a fan without confirmation from the individual or organization … The individual or organisation can delete any message posted by third parties.' His Honour explained that on Twitter, 'Tweets are publicly visible by default, although senders can restrict message delivery only to certain users' 39.

[896] *HL (A Minor) by her Father and next friend AL v Facebook Inc, & Anor* [2013] NIQB 25. At that time Facebook was described as having over 900 million active users worldwide; 3.2 billion comments per day; and 'open' privacy settings to registered users who declare they are over 18 years of age [14]. The plaintiff was a 12 year old, 'particularly vulnerable young lady', subject to an Interim Care Order who had continually absconded over a two year period and was found consuming alcohol and drugs in the company of older males. She had been engaged in 'posting and/or uploading sexually suggestive and/or inappropriate photographic images of herself, together with self-orientated literary content, on the Facebook social network website' [5]. The claim was that Facebook had failed to prevent her access to this social network site and had failed to require age and identity verification or express parental consent due to an inadequate monitoring system. His Honour considered that relief could not be granted in this case due to the 'inefficacy of the remedy sought' [25].

[897] *HL (A Minor) by her Father and next friend AL v Facebook Inc, & Anor* [2013] NIQB 25 at [16].

[898] Social Media News reported that there were 316 million active monthly users of Twitter worldwide in September 2015, with 500 million Tweets being sent every day, 80% of those were reported as mobile users: <https://about.twitter.com/company>. By February 2017 it was reported that there were 2,800,000 monthly active Australian Users of Twitter <https://www.socialmedianews.com.au>.

[899] *Chambers v Director of Public Prosecutions* [2013 1 WLR 1833, 1836. The appeal was allowed in this case because the tweet was not found to be of a 'menacing character' within the meaning of s 127(1)(a) of the *Communications Act 2003* (UK). For further details of this case see discussion on page 169 of this thesis.

[900] *Chambers v Director of Public Prosecutions* [2013] 1 WLR 1833, 1836.

recent tweets. Tweets can be addressed to a specific user and can also be viewed by followers, however, non-users can search for tweets of interest and non-followers can access the public time lines. There can be links to YouTube, an interactive video channel that allows users to upload, view and share videos, to enhance the information available in 140 characters.[901] It offers both public and subscription channels with restricted viewing for subscribers.[902]

Other OSNs are limited and restricted to targeted groups with increased ontological friction and a greater protection for personal data. These include networks such as Legal OnRamp, LinkedIn and Martindale-Hubbell Connected. Legal OnRamp is a referred to as a collaboration system for in-house counsel and invited lawyers and third party service providers and is directed at a limited class of lawyers.[903] It provides an opportunity for members to ask questions of other lawyers, share documents, obtain referrals for clients and find resources. Legal OnRamp is a leading legal Web 2.0 platform. It is not restricted to large firms and has been seen as an opportunity for smaller firms to demonstrate that they can manage specialised areas of work.[904] LinkedIn[905] is promoted as the 'world's largest professional network' with links to Twitter, Facebook and YouTube.

Martindale-Hubbell Connected is a closed online community of lawyers, paralegals, corporate council and other legal professionals which uses collaborative tools to assist lawyers to share opinions in a secure area by the private messaging feature. While it has many features in common with other social networks, it is an exclusive network on secure platforms. Membership is restricted mainly to inhouse lawyers and by invitation. Both Legal OnRamp and Martindale-Hubbell Connected are collaborative platforms and have been viewed by the Michigan Bar Journal as 'viable avenues for client communication' as well as an opportunity for in-house counsel to ask questions and discuss 'hypothetical dilemmas'. [906]

[901] You Tube <http://www.youtube.com>.
[902] See discussion of specific use of You Tube by Australian courts in this thesis at page 147.
[903] Legal OnRamp was founded in 2007 by the legal technology company OnRamp Systems and claims to be used by lawyers from 40 countries. In 2016 it was acquired by Elevate Services, a global legal service provider of 'strategy, operations, technology and talent' to corporate legal departments and law firms <http://legalonramp.com>.
[904] Brett Burney, 'Meeting Your Clients on the Ramp' (June 2010) *Michigan Bar Journal* 60-61, 61. This article reported that in 2010 there were over 11,000 members with active forums and groups which are either public or private.
[905] LinkedIn was launched in December 2003 and claims to have more than 300 million registered users worldwide, <https://linkedin.com>.
[906] Martindale-Hubbell Connected <http://community.martindale.com>.

The restricted and closed networks offer more control over membership and content and may be more suitable for legal dialogue, however, such restricted networks do not engage with the general public. More open networks, such as Twitter, offer more opportunities for facilitating access to justice due to the greater number of people who can be reached, however, the reduction of 'ontological friction'[907] and the rapid flow of personal information within the OSNs environment can threaten privacy and lead to a reluctance by many to participate.

4.3 Online social networks: enhancing access to justice

4.3.1 Introduction

Substantial benefits have been identified for lawyers and courts using OSNs, particularly for direct communication, improving transparency and for making the legal system more accessible. In a relatively early assessment of OSNs, Susskind considered that its impact on the legal system was limited, except for the use of Facebook and MySpace by human resources departments, to surveillance of actual and potential employees and for use as business tools for law firms.[908] The use of LinkedIn was distinguished because of its focus on professional and business users.[909] The closed community, LegalOnRamp[910], was viewed as most promising for the legal profession, being more secure and like 'a cross between Facebook and Wikipedia'.[911]

However, attitudes to OSNs have changed. They have been viewed as providing 'a platform for legal professionals to promote the administration of justice, by engaging the public in legal practice and debate' and they offer 'access to a vast audience and resources such as real-time legal updates and the ability to discuss these with legal practitioners internationally'.[912] They have also become a new area requiring legal advice for clients, particularly in defamation and employment law, due to the public nature of the disclosure and limited control provided to users of OSN in wide dissemination of third party posts.

[907] Floridi, above, n 548, 185-187. Floridi explains that '*informational privacy is a function of the ontological friction in the infosphere'* so that if there is more personal information available in the environment, the ontological friction will be lower and the accessibility of this personal information higher. He uses an example of a brick wall which provided higher 'ontological friction' for the flow of acoustic information than paper-thin partitions.
[908] Susskind, above n 55, 78.
[909] Ibid.
[910] Legal OnRamp is a collaboration system for in-house counsel, invited lawyers and third party service providers. Lawyers from over 40 countries participate <http://legalonramp.com> .
[911] Susskind, above n 55, 79-80.
[912] International Bar Association, *IBA International Principles on Social Media Conduct for the Legal Profession* (adopted, 24 May 2014) <www.ibanet.org> 2.

The three characteristics of OSNs that sharply contrast with characteristics of the judicial system that will need to be reconciled before OSNs can offer improved access to justice have been identified as:

> 1. New media are decentralized and multidirectional while the courts are institutional and unidirectional.
> 2. New media are personal and intimate while the courts are separate and, by definition, independent.
> 3. New media are multimedia, incorporating video and still images, audio and text, while the courts are highly textual. [913]

These represent 'unique incongruities' that the courts will need to overcome to use OSNs effectively to improve access to justice online.[914]

I will first consider the advantages OSNs can offer by facilitating the flow of information and offer numerous opportunities for courts in making them more accessible, encouraging transparency and engagement[915] and then I will discuss the disruption they provide in the regulatory environment.

4.3.2 Opportunities for the courts

The substantial benefits promised by OSNs relate to the issue of accessibility which is dependent on the 'ontological features'[916] of their specific environment. It is an environment created to facilitate the flow of personal information with a more limited degree of "'ontological friction" regulating the information flow within the system'.[917].

The increasing accessibility provided by OSNs can enhance direct communication between the public and the courts; provide information and opportunities for public education, and improve transparency and confidence in the legal system. They also assist litigation and court processes as they have become a fruitful source of evidence for litigation and have proven to be useful for the service court documents.

[913] Executive Summary, Conference of Court Public Information Officers, 'New Media and the Courts: The Current Status and a Look at the Future' (26 August, 2010) A Report of the Conference of Court Public Information Officers: In Partnership with the National Center for State Courts and The E W Scripps School of Journalism at Ohio University, 8 <http://www.ccpio.org>.
[914] Ibid.
[915] Legal Projects Team, *The Impact of Online Social Networking on the Legal Profession and Practice* (Report, International Bar Association, February 2012) 33 <http://www.ibanet.org>.
[916] Floridi, above n 561.
[917] Ibid 186. Floridi explains that 'ontological friction' refers to the forces that oppose the information flow within (a region of) the infosphere.

By the use of OSNs, people can be provided with the means to ask questions about court procedures and processes and use live chat facilities such as offered by the Family Court of Australia on the court's website,[918] although people need access to the internet, technical literacy and a willingness to engage with the Family Court in this way. The live chat facility is publicised on the Court's Twitter account and encourages people to use the chat facility to communicate with the Court.[919]

The Australian courts using Twitter have indicated that they are providing information about court processes, seminars, special tours, links to articles[920] and special programs targeting youth education. The Family Court Tweets offer information such as 'Tips for going to court'[921]; information on applying for consent orders,[922] issuing a subpoena[923] and new eServices[924]; details about children and international travel after family separation; and information on issues of public importance such as domestic violence.[925] The judgment and summary of numerous cases of public interest on video can be accessed from the Federal Court website.[926]

Information is also readily available on YouTube. It is used by courts in Australia, Europe, US and UK to provide educational materials as well as information about cases and processes for court filings. Its content is often linked to Twitter posts to enable detailed explanation of events. Some content is restricted and access is only available through the organisation's approval. The High Court of Australia has made public audio-visual recordings of its hearings from 1 October 2013 to improve public access to its hearings. The recordings are available a few business days after the hearings to ensure there is time for vetting of materials for information that may be the subject of publication constraints. The recordings do not include

[918] The live chat facility offers help with Family Law through an online chat facility. The chat facility is with an agent of the court if the person has a procedural family law question or queries about eFiling on the Commonwealth Courts Portal <http://www.familycourt.gov.au>.

[919] The Family Court twitter account announcement states: 'Avoid the phone queen! Chat online instantly with the National Enquiry Centre' and can be found at <https://twitter.com@FamilyCourtAU>.

[920] Family Court Tweet on 10 September, 2015 – link to Justice Strickland's paper examining recent decisions concerning gender diverse youth <https://twitter.com@FamilyCourtAU>.

[921] The Tweet on 3 August, 2015 includes a link to the Family Court website and the publication on preparing for a court hearing <https://twitter.com@FamilyCourtAU>.

[922] Family Court Tweet on 9 August 2015 <https://twitter.com@FamilyCourtAU>.

[923] Tweet by the Family Court on 13 August 2015 <https://twitter.com@FamilyCourtAU>.

[924] Family Court Tweet, 6 September 2015 <https://twitter.com@FamilyCourtAU>.

[925] Family Court on Twitter, 21 September 2015 announcing the report, *Stepping Stones,* by Women's Legal Service Victoria on family violence and financial hardship faced by women, <http://www.womenslegal.org.au> ; as well as retweets on 17 September 2015 <https://twitter.com@FamilyCourtAU>.

[926] Federal Court of Australia website <http:www.fedcourt.gov.au>.

applications for Special Leave but otherwise cover all Full Court hearings in Canberra.[927] Examples of Federal Court of Australia videos on YouTube include: *Mediation in the Federal Court of Australia* which demonstrates the process of mediation and has over 1,100 views; and judgment summaries, including high profile cases such as *Seven Network Limited v News Limited*[928] and *National Rugby League Investments Pty Limited v Singtel Optus Pty Ltd.*[929]

The efforts by the Family Court of Australia to increase transparency using OSNs can be appreciated in the context of the tensions created by the competing demands of transparency and privacy, confidence and confidentiality which are essential in family law, particularly for the protection of children. This was a central issue of a report on UK courts which proposed to open 'the family court while ensuring that we protect the privacy of the personal lives of those involved in family proceedings – particularly children'.[930] The openness, discussed in detail in Chapter Two of this thesis, and reporting on court proceedings has been regarded as essential for transparency and for maintaining public confidence in the courts. This public confidence can be established through public scrutiny also protects against accusations of bias and discrimination which is harder to defend when courts operate 'behind closed doors'.[931] The Family Court of Australia began using Twitter from October 2012 and by 27 February 2014 they had launched their Official YouTube channels to provide informational videos[932] to assist particularly unrepresented litigants with court procedures. YouTube has added to the courts'

[927] High Court of Australia website <http://www.hcourt.gov.au> media release>.

[928] *Seven Network Limited v News Limited* [2007] FCA 1062. In this case Seven Network Limited claimed that it had to shut down C7 Pty Ltd's business in the production and distribution of sports channels for Australian pay television platforms because some of the respondents engaged in anti-competitive conduct in contravention of ss 45 and 46 of the *Trade Practices Act 1974* (Cth) between 1999 and 2001. The case was described by Justice Sackville as '*meta-litigation*'. The trial lasted for 120 hearing days in an electronic courtroom where 12,849 '*documents*' were admitted into evidence. There were 9,530 pages of transcript of the trial. His Honour estimated that the parties spent $200 million on legal costs which Sackville J considered 'not only extraordinarily wasteful but borders on the scandalous'. The applicant claimed $1.1 billion in damages. The judgment is about 1120 pages in length.

[929] *National Rugby League Investments Pty Limited v Singtel Optus Pty Ltd* (2012) 201 FCR 147. This case concerned the copyright in broadcasts of a number of Australian Football League (AFL) and National Rugby League (NRL) games in September and October 2011. The rightholders (the AFL, NRL and Telstra which had an exclusive licence from the AFL and NRL to exploit free to air broadcasts of live and pre-recorded games on the internet and mobile telephony) claimed that the applicants had breached their copyright.

[930] Consultation Paper CP11/06 Department for Constitutional Affairs, Justice, rights and democracy, *Confidence and confidentiality: Improving transparency and privacy in family courts* 'Foreword' Lord Falcone, Lord Chancellor and Secretary of State for Constitutional Affairs and Harriet Harman QC MP, 6.

[931] Ibid 34.

[932] The YouTube channel <www.youtube.com/familycourtAU> provides videos such as *How to apply for a divorce: serving divorce papers*.

use of Twitter since the introduction of Twitter Cards[933] which have made the addition of photos and videos on Twitter commonplace.[934]

Since 2013 in South Australia it has been possible for lawyers and the media to tweet and blog from the Supreme Court, reporting directly on criminal verdicts and important civil cases, with some limitations, such as a fifteen minute time delay in publication to allow for review. Chief Justice Chris Kourakis considered that this was made possible due to a demand from journalists and reflected a change in communications and the need to provide information more quickly. The Chief Justice explained that as people expect information quickly, the courts have an obligation to provide it unless it interferes with the administration of justice.[935]

Statements, often relating to matters of high public interest, which were previously issued in media releases or published through court media liaison officers can now be made available on OSNs by the courts. The public and the media do not have the same level of access to family courts as there are restrictions on how court proceedings are recorded and what information can be published and broadcast, including on OSNs.[936] The Chief Justice of the Family Court issued a media release in 2011 to clarify the media coverage of a serious incident involving a father protesting on the top of the Sydney Harbour Bridge. Her Honour found that the media speculated that such an incident was caused by a disgruntled party dissatisfied with court orders. There was, however, no current or past proceeding concerning parenting or custody arrangements for this person in the Family Court.[937] Such information could be distributed more quickly using OSNs.

Twitter has been found to be the most popular OSN tool for courts in the US where its use has spread. For many it has 'become a mainstay for communicating critical, time-sensitive information to the public and the media'.[938] The main uses of Twitter were found to be for

[933] <https://dev.twitter.com/cards/overview>.

[934] See Tweets: 21 September 2015, photo with Chief Justice Bryant, Rosie Batty and Martin Pakula MP; photo on 7 September 2015 taken at the awards for Court Network volunteers who provide invaluable support to clients in the family law courts.

[935] Loukas Founten and Candice Marcus, 'Tweeting to be allowed from South Australian courtrooms' *ABC News* (online), 9 September 2013 <http://www.abc.net.au/news/2013-09-09/tweeting-twitter-allowed-from-south-australian-courtrooms/4945520>.

[936] Section 121 *Family Law Act 1975* (Cth) makes it an offence to publish proceedings or images that identify people involved in family law proceedings or images that identify people involved in family law proceedings unless a Publication Order has been made or another s 121 exemption applies.

[937] Chief Justice Diana Bryant, Media release, Family Court of Australia (online) 20 May 2011 <http://www.familycourt.gov.au>.

[938] CCPIO Report, above n 882, 12.

providing information to the public about routine matters such as physical access to the courtroom and logistical issues; releasing decisions; announcements about upcoming oral arguments; for retweeting news from other courts or organizations; providing responses to individuals where possible; targeting the younger 'electronic-only generation'; reviewing what employees are saying about their work; and to follow other courts and news organizations.

A 'strong interest was found in using online social media to communicate court decisions and engage with the community' by the Supreme Court of Victoria and the Family Court of Australia using Twitter, Facebook and YouTube.[939] Former Chief Justice John Doyle considered that the courts 'are well placed to explain their function'[940] to provide access to the courts and so maintain public confidence in the system of justice by enabling the public to observe and understand what the courts are doing'.[941] He considered that the courts should play a proactive role and should 'try to reach those who choose not to exercise the right of access in person and to inform them of what the courts are doing and why they do it' in order to fulfil the obligation to earn public confidence in 'our system of justice'.[942] With the application of Web 2.0 tools the means of providing an explanation of the function of courts is available and it is no longer necessary for courts to 'acquire their credibility and account to the wider community' through the media, as was previously suggested.[943] The judgment and summary of numerous cases of public interest on video can be accessed from the Federal Court website for those unable to attend court in person.[944]

More recently some court documents have been served using OSNs, however this has not yet become common practice. The procedure has been mainly used for substituted service when the judge has been satisfied that the Facebook profiles were those of the defendant. Courts will not permit substituted service[945] through OSNs unless they can be satisfied that there is sufficient

[939] The Family Court of Australia has 11 videos on YouTube with 185 subscribers. These videos describe eFiling, mediation; they provide information for children 5-8 yrs and 9-12 yrs about what it means to see a family consultant, and provide a tour of the court <https://www.youtube.com/user/familycourtAU> .

[940] The Hon Justice John Doyle 'The Courts and the Media: What Reforms are Needed and Why?" (1999) 1 *UTS Law Review* 25-31, 27.

[941] Ibid 26.

[942] Ibid.

[943] Roderick Campbell, 'Access to the Courts and Its Implications' (1999) 1 UTS Law Review 127-135, 131.

[944] See <http://www.fedcourt.gov.au/publications/judgments/judgment-summaries> and <http://www.fedcourt.gov.au/publications/videos>.

[945] Application for substituted service in *Citigroup Pty Limited v Weerakoon* [2008] QDC 174 was made pursuant to Rule 116(1) of the *Uniform Civil Procedure Rules 1999* (Qld) which permits substituted service when it is impracticable to serve a document as required.

connection between the Facebook page and the defendant. In *Citigroup Pty Limited v Weerakoon*[946] Judge Ryrie was 'not so satisfied in light of looking at the – the uncertainty of Facebook pages, the facts that anyone can create an identity that could mimic the person's identity'.[947] While Ryrie J considered that 'practically speaking' the Facebook page might be the defendant's, however, his Honour expressed concern about the 'uncertainty' of Facebook pages and 'that anyone could create an identity that could mimic the true person's identity'. On the facts of this case Ryrie J found that some of the information did not demonstrate 'with any real force that the person who created the Facebook page might indeed be the defendant'. His Honour ordered that personal service be dispensed with because there was a practical impossibility of personal service but there was an alternative to request for service via the Facebook page. Substituted service was to be effected by posting the relevant documents to the post office box, the last known postal address of the defendant and one that had previously been found to be a reliable contact address.

By contrast in *Symes v Saunders*[948] Judge Robin QC of the Queensland District Court permitted substituted service of an application for criminal compensation because the judge was satisfied that the respondent 'received' the application which was acknowledged and discussed with the applicant's solicitor. The respondent had been contacted by the applicant's lawyer on Facebook and on his mobile phone and the respondent was informed of the court listing. His Honour considered that the applicant's lawyer deserved 'some commendation for his initiative' in using an alternative method of substituted service rather than a newspaper advertisement when no current address for the respondent had been found. Judge Robin QC expressed concern that this alternative method 'not approved by the court' was used, however the matter proceeded 'in the interests of efficiency' and to save further costs.

When the plaintiff could not be located for personal service of documents in *MKM Capital Pty Ltd v Corbo & Poyser*[949], a default judgment was served on Facebook using a private message. In that case, Master Harper was satisfied that the defendants could not be located and the Facebook profiles belonged to the defendants. Substituted service by Facebook was also ordered in *Byrne & Howard*[950] after evidence was submitted about the respondent's Facebook

[946] *Citigroup Pty Limited v Weerakoon* [2008] QDC 174.
[947] *Citigroup Pty Limited v Weerakoon* [2008] QDC 174.
[948] *Citigroup Pty Limited v Weerakoon* [2011] QDC 217.
[949] *Capital Pty Ltd v Corbo & Poyser* Unreported, ACT Supreme Court, Master Harper, 12 December 2008.
[950] *Byrne & Howard* (2010) FLR 62.

page, his use of the site and the electronic confirmation of receipt of documents. The Federal Magistrate also considered the provisions of the *Family Law Rules 2004* and the provisions relating to substituted service. Keyzer et al considered that Australian courts by using OSNs could 'improve service of process, generate vital evidence in civil cases, and track down perpetrators of crime'.[951] Cases in Australia, the US and the UK have indicated that whether Facebook or other social networking sites are used for the service of documents will be decided on a case by case basis. [952] Factors that have been considered include; the authentication of the Facebook profile; the difficulties encountered with personal service; whether the account is active and accessed regularly by owner; whether it is be reasonably likely that person would log on and check the account; and whether it is reasonably likely that the account is owned by the person concerned.

Robertson has argued that social media will improve access to justice for 'middle class litigant' who may not have access to legal representation but can access social media.[953] This use of social media was seen as facilitating access to justice by enabling self-represented litigants to collect evidence outside the court mechanisms of discovery;[954] by providing access to 'the wisdom of the crowds'; by providing access to services which will assist in the preparation of legal documents; and finally by connecting litigants to limited services overseas at reduced rates.[955]

Evidence found on OSNs has also been significant in employment law cases. In *Lukazsewski v Capones Pizzeria Kyneton*[956] the respondent lodged a motion for dismissal of Lukazsewski's application on the grounds that was frivolous, vexatious or lacking in substance. Mr Lukzsewski's employment had been terminated on the basis of a Facebook entry which indicated he was 'pissed off'. He claimed that his employment was terminated without payment

[951] Keyzer et al, above n 873, 50-51.

[952] In the US in *Mpage v Mpafe* MN No 27-FA-11-3453, service of divorce proceedings were allowed by Judge Kevin Burke by email, Facebook, Myspace or any other social networking site to ensure that service was effective and cheaper and the respondent was found; in *Fortunato v Chase Bank USA* 2012 WL 208950, 2 (S.D.N.Y) (*Fortunato)* Judge Keenan found that the applicant had not provided any evidence that the Facebook profile was used by or maintained by the respondent; In *Federal Trade Commission v PCCARE247 Inc* 2013 WL 841037, 2 (S.D.N.Y.) Judge Engelmayer distinguished *Fortunato* because there was sufficient evidence that the Facebook accounts were owned by the defendants. In the UK in *Blaney v Persons Unknown* (October 2009, unreported) Twitter was used to serve an injunction on an anonymous defendant who had been impersonating the plaintiff. In Australia, in *Mothership Music Pty Ltd v Ayre* [2012] NSWDC 42, substituted service on Facebook was ordered, however this was successfully appealed in the New South Wales Court of Appeal in *Flo Rida v Mothership Music Pty Ltd* [2013] NSWCA 268 because it was considered that there was no evidence that the service by Facebook would have been brought to the defendant's attention while he was in Australia.

[953] Robertson, above n 860, 6.

[954] Ibid 81-83.

[955] Ibid 10-20.

[956] *Lukazsewski v Caponnes Pizzeria Kyneton* [2009] AIRC 280.

in lieu of notice due to the Facebook post, however this did not have a specific reference to his employment and was not directed to a particular person. The motion was dismissed and the matter proceeded to conciliation. In *Dover-Ray v Real Insurance Pty Ltd*[957] the applicant had written a blog on an OSN, MySpace which was publicly accessible and had the potential to damage the respondent's reputation. It was held that there was a valid reason for terminating the applicant's employment due to the publication of the blog and not modifying or removing it and in addition distributing emails with pornographic photographs.

Blackham and Williams identified a number of key opportunities for courts in using online social networks: the first, that their use may make the courts more accessible and responsive to users; secondly, they can be used in an educative role by facilitating people's engagement with the court and their understanding of court processes; thirdly, by encouraging engagement with the courts they may promote transparency and help to 'prevent corruption'; and fourthly; by providing courts with a direct channel of communication provide 'a voice' and an opportunity for courts to counteract adverse media reporting.[958] They also considered that the courts could use OSNs to 'build more personal relationships with individuals and thereby show a more "human" side to the judicial system'.[959]

It is this personal relationship and human side of the judicial system exposed by OSNs which paradoxically has the capacity to enhance access to justice and diminish it. This can be described within the framework provided by Floridi and is due to the 'technologies of self construction'[960] with the subsequent transformation of the 'onlife' experience or 'the fourth revolution' in self-understanding in a 'new environment' or 'infosphere' where the distinction between 'online and offline will become blurred'.[961] This is disruptive for the legal regulatory environment when both online and offline personal data have become integrated. Therefore, as Blackham and Williams also discussed, the engagement with new technologies 'may affect the integrity of the courts and reduce public confidence in judicial processes' by exposing the courts to criticism or jeopardising the due administration of justice.[962] It is the degree of detachment,[963]

[957] *Dover-Ray v Real Insurance Pty Ltd* (2010) 204 IR 399.
[958] Blackham and Williams above n 848, 210.
[959] Ibid.
[960] Luciano Floridi, 'The Informational Nature of Personal Identity' (2011) 21 *Minds & Machines* 549-566, 550.
[961] Floridi, above n 862, 477.
[962] Blackham and Williams, above n 875, 210-211.
[963] *Dennis v United States* (1951) 341 U.S. 494, 525. Justice Frankfurter, concurring in this case explained the essential quality of courts is their 'detachment, founded on independence'. They are not representative bodies nor are they 'designed to be a good reflex of a democratic society'.

antithetical to the inherent characteristics of OSNs, that has been seen to protect the authority of the courts.

4.4 Disrupting the legal regulatory environment

4.4.1 The general nature of the disruption

The reluctance of courts to adopt OSNs for communication can be attributed to an inherent conflict of cultures –the highly regulated and controlled legal culture which has been confronted by a largely unregulated and evolving one.[964]

The significant disruption identified by Chief Justice T F Bathurst was that:

> The **rule of law** is being challenged by social media … it reveals the vulnerability we open our civilization to by integrating social media into our lives before the rule of law has been integrated into it.[965]
> (emphasis added)

Two relatively recent cases heard in the High Court of Justice of Northern Ireland by Justice McCloskey refer to this challenge to the rule of law by infringing posts on Facebook.[966] Both cases concerned requests for anonymity orders. His Honour referred to the governing principles concerning anonymisation and the 'overarching principle of open justice'.[967] These factors included consideration of risk to the applicant's access to justice which may have been thwarted without anonymity. His Honour also considered that this case served 'as a timely reminder that we live in a society governed by the rule of law'[968] and granted the plaintiff injunctive relief to protect him from further unlawful conduct. Facebook was required to remove the offending page from its website which was considered unlawful harassment. Justice McCloskey found that, while OSNs 'can be a force for good in society', they are being

[964] See features of 'incompatibility' discussed previously, 145.

[965] T F Bathurst, 'Social Media: The End of Civilization? (Paper presented at the University of New South Wales for the Warrane Lecture,, Sydney, 21 November 2012) 29.

[966] The cases are: *XY v Facebook Ireland Limited* [2012] NIQB 96 and *AB Limited, JW, SM and CM v Facebook Ireland Limited and A Person or Persons Adopting the Pseudonyms Ann Driver and Alan Driver* [2013] NIQB 14. *XY v Facebook Limited* concerned the posting of a page 'Keeping Our Kids Safe From Predators' on Facebook which contained detailed information about a sex offender who had 15 convictions when he was a juvenile and an unauthorized photograph. It also contained threats and details about his ill health. The judge considered this Facebook page to be *'prima facie,* unlawful harassment', threatening the plaintiff's right to respect for private and family life and rights to freedom from inhuman and degrading treatment.

[967] *XY v Facebook Ireland Limited* [2012] NIQB 96 at [4] his Honour held that '[i]n the present case, the main factors to be balanced are the nature and extent of information pertaining to the Plaintiff's identity already in the public domain, the accessibility of such information, the risk that the Plaintiff's access to justice will be thwarted if anonymization is not granted, the Plaintiff's right to freedom from inhuman or degrading treatment and the Plaintiff's right to respect for his private and family life'. Justice McClosky also considered that granting anonymity 'would constitute a relatively modest dilution of the principle of open justice'.

[968] *XY v Facebook Ireland Limited* [2012] NIQB 96, [13].

'increasingly misused as a medium through which to threaten, abuse, harass, intimidate and defame' and with this 'misuse of social networking sites and the abuse of the right to freedom of expression' marching together[969] they have become the "'wild west" of modern broadcasting, publication and communication'.[970] His Honour considered that 'the solution to this mischief' was not clear and 'beyond the powers of this Court', perhaps lying in '[s]elf-regulation and/or statutory regulation'.[971]

In *HL (A Minor) By her Father and Next Friend, AL*[972] McClosky J found that the interim application for injunctive relief in this case could not succeed. His Honour accepted the plaintiff's willingness and ability to engage in inappropriate behaviour was not dependent on access to Facebook and that Facebook had 'no efficacious mechanisms for preventing access to its site. Facebook admitted 'that it has created something of a monster which, it alleges, it cannot control'.[973] His Honour considered that this 'plea of impotence' by Facebook would be the subject of judicial scrutiny in the future.[974] Justice McCloskey acknowledged that in such a time of rapid change, 'jurisprudence in this sphere is both dynamic and evolving'.[975]

The liability of OSNs such as Facebook for posts has been challenged in many jurisdictions, particularly the regulatory role such organisations perform.[976]

[969] *AB Limited, JW, SM and CM v Facebook Ireland Limited and A Person or Persons Adopting the Pseudonyms Ann Driver and Alan Driver* [2013] NIQB 14 at [13].
[970] *AB Limited, JW, SM and CM v Facebook Ireland Limited and A Person or Persons Adopting the Pseudonyms Ann Driver and Alan Driver* [2013] NIQB 14 at [13].
[971] *AB Limited, JW, SM and CM v Facebook Ireland Limited and A Person or Persons Adopting the Pseudonyms Ann Driver and Alan Driver* [2013] NIQB 14 at [14].
[972] *HL (A Minor) By her Father and Next Friend, AL* [2013] NIQB 25. This case concerned a 12 year old girl who had been engaged in posting and uploading sexually suggestive and inappropriate photos of herself and accompanying text on Facebook, using several different account with different profile names. The girl was the subject of an Interim Care Order due to continually absconding, consuming alcohol and drugs in the company of older men. Her father was attempting to prevent her access to Facebook.
[973] *HL (A Minor) By her Father and Next Friend, AL* [2013] NIQB 25 at [24].
[974] *HL (A Minor) By her Father and Next Friend, AL* [2013] NIQB 25 at [24].
[975] *HL (A Minor) By her Father and Next Friend, AL* [2013] NIQB 25 at [26] McCloskey J referred to the decision in *Tamiz v Google* [2012] EWHC 449 where it was found that Google was neither a publisher nor an entity which authorizes publication but has a passive role as a platform provider.
[976] In *Stuart Force & Anor v Facebook, Inc* United States District Court, Southern District of New York, Case 1:16-cv05490. Complaint the plaintiffs, the families of five Americans murdered or injured in Palestinian terror attacks, alleged that Facebook knowingly provided material support and resources to Hamas, a 'notorious terrorist organization' by permitting posts such as a page entitled 'Death to Zionist baby killer Israeli jews [sic]' and an image of the Israeli Prime Minister as a vampire with blood dripping down his chin as he feasted on a child. Facebook initially declined to remove the posts because the company considered they did not violate their community standards. It was alleged that Facebook could monitor and block such material because the algorithms they use provide considerable control over the material published and therefore the company was responsible for intentionally assisting HAMAS in its terrorist attacks. The claim is for $1 billion in punitive damages.

4.4.2 OSNs diminishing access to justice?

OSNs have been found to have had considerable impact on courts.[977] They have presented a challenge for courts because of the instantaneous nature of their communication and the freedom provided for unrestricted comments. They have been seen as possibly dangerous to the integrity of the courts and to have the potential to interfere with the trial process.[978] They have the potential to diminish access to justice by transforming the transparency online to overexposure.

The free flow of information on OSNs has led to cases being decided on information and evidence not produced in court. This has reached a new dimension in many cases where jurors regard such interactive discussion of personal and public issues acceptable and commonplace. The widespread use of OSNs has made the task of ensuring a fair trial for an accused in the digital era more difficult, particularly for jury trials. The increasing incidence of juror misconduct was cited as a reason more research and innovation is needed into ways the jury system can adapt and survive the challenges of social media.[979] It has been argued that the anonymity and immediacy of social media encourages the search for additional information.[980]

Tweeting about jury duty has been become an active pastime. The availability of smart phones has exacerbated the level of juror misuse of social networks by making it easier for people to comment on court proceedings.[981] Research using the Twitter hashtag[982] *#juryduty* found numerous Tweets from jurors discussing their jury service, some linking to photographs on Instagram or Twitter[983]. Some of the examples discussed included:

> Hangman, hangman slack your rope. #juryduty

[977] Emily M Janoski-Haehlen, 'The Courts Are All a ""Twitter": The Implications of Social Media Use in the Courts' (2011) 46 *Valparaiso University Law Review* 43.
[978] Ibid 44.
[979] Marilyn Krawitz, 'guilty as Tweeted: Jurors Using Social Media Inappropriately During the Trial Process', University of Western Australia – Faculty of Law Research Paper No. 2012-02.
[980] Peter Lowe, 'Jury 2.0' (2011) 62 *Hastings Law Journal* 1579, 1613.
[981] Marcy Zora 'The Real Social Network: How Jurors' Use of Social Media and Smart Phones Affects a Defendant's Sixth Amendment Rights' (2012) *University of Illinois Law Review* 609.
[982] A hashtag on Twitter using # marks key words or topics. It is used to create categories of conversations and it makes it easier for users to search particular topics.
[983] Hon Antoinette Plogstedt, 'E-Jurors: A view from the Bench' (2013) 61 *Cleveland State Law Review* 597, 603-604 and 645, Appendix A: Sample #JURYDUTYTweets, April 30 – 3 May 2013).

> Every time a witness completes their testimony, I feel like clapping for their performance. #juryduty.
>
> Just started #juryduty. Decided to start forming opinions on the trial now to save time.#guilty!#nodickingaround[984]

Judge Plogstedt found that there were several areas of concern: the first that jurors were conducting their own research; secondly, they were communicating with people outside the courtroom about the case; and thirdly, they were engaging in 'pre-deliberation discussions with each other'.[985] Her Honour concluded that courts need to 'frequently revisit methods of preventing and monitoring electronic jury misconduct'[986] to ensure that there will be less likelihood of juror misusing OSNs.[987]

Twitter was viewed by Lee as the new source 'digital misadventures'[988] for jurors which endanger the 'sanctity of the trial'[989] because it incorporates more instantaneous, focussed conversation with shared experiences and external comment in 'rapid-fire'[990] from the 'palm of the juror's hands'.[991] She considered that the current preventative measures fail because they are not uniform or specific, lack policy reasons and are not provided in writing and orally to assist jurors. Banning technology from the courtroom was seen as frustrating and of limited use because jurors are still able to access technology during breaks from the trial or at home. [992]

More recently, in September 2015 Anna Kendrick, an American actress and singer was reported as having 'spent a whole day hilariously live-tweeting her jury duty'.[993] Some of her Tweets were:

> Night 3 of calling in for jury duty … thought I was off the hook, but I've got a date with justice … and the bitch wants an early morning tryst @AnnaKentrick47
>
> Holy shit. Got called, but as we were walking to the courtroom they settled the case. Which I didn't know was a thing. #WorkItOut#jury duty

[984] Ibid.
[985] Ibid 598.
[986] Ibid 639.
[987] Ibid 644.
[988] Laura Whitney Lee, 'Silencing the "Twittering Juror": The Need to Modernize Pattern Cautionary Jury Instructions To Reflect the Realities of the Electronic Age' (2010-2011) 60 *DePaul Law Review* 181-222.
[989] Ibid 181.
[990] Ibid 182.
[991] Ibid 184.
[992] Ibid 206.
[993] Rob Moran, 'Anna Kendrick spent a whole day hilariously live-tweeting her jury duty' (30 September 2015) <http://www.dailylife.com.au/dl-people/dl-entertainment/anna-kendrick-spent-a-whole-day-hilariously-livetweeting-her-jury-duty-20150929-gjxpqq.html>.

Jurors have exchanged Facebook messages with parties,[994] divulged details of an ongoing trial,[995] commented on a trial after it has concluded[996], sought advice about a trial,[997] 'friended' each other on Facebook and generally used the internet to gain information about the accused. The issue of juror 'research' was addressed by Lord Chief Justice Judge in the United Kingdom in *R v Karakaya.*[998] His Honour considered that this 'research' contravened the rule of law and it contravened two linked principles: the first, because the defendant, particularly, is entitled to know of the 'evidential material considered by the decision making body'[999] and the second principle, that the prosecution and defence are entitled to an 'opportunity to address all the material considered by the jury'.[1000]

Bromberg-Krawitz recommended that Australian courts should address the issues associated with the use of social media which threaten the right to a fair trial and implement preventative measures.[1001] She referred to the decision in *Haruna v The Queen*[1002] where the Court of Appeal of Western Australia held that the primary judge was correct in discharging the foreperson of the jury for communicating, during the course of the trial, with a lawyer from the office of the Director of Public Prosecutions (Western Australia) via text message and Facebook about certain aspects of the trial, contrary to instructions given to the jury at the commencement of the trial.[1003]

Before the rapid expansion of Twitter use, considerable faith in the integrity of juries and 'their capacity to understand and adhere to directions' was expressed by Justice Weinberg in *R v Dupas*

[994] *A-G v Fraill* [2011] EWCA Crim 1570, [2011] 2 Cr App R 21.
[995] Digital Media Law Project, Harvard, *California Bar v Wilson* 23 January 2009 <http://www.dmlp.org>.
[996] *Commonwealth v Werner* 81 Mass App Ct 689 (2012), February 1, 2012.
[997] UK juror dismissed from a child abduction and sexual assault trial.
[998] *R v Karakaya* [2005] Cr App R 5 at [24]-[25]. In this case the jury bailiff found documents downloaded from the internet in the jury room after the verdict had been reached.
[999] *R v Karakaya* [2005] Cr App R 5 at [24]. page
[1000] *R v Karakaya* [2005] Cr App R 5 at [24].
[1001] Marilyn Krawitz, *An Examination of Social Media's Impact on the Courts in Australia* (PhD Thesis, Murdoch University, 2014) 3, 242-243.
[1002] *Haruna v The Queen* (2013) 278 FLR 194.
[1003] *Haruna v The Queen* (2013) 278 FLR 194, 197-198. Communications on 15 March 2012 included: 'Yea it's reasonably interesting-the refugee stories fascinate me…and the mong comments from other jurors always keeps me entertained haha, whilst terrifying me at the same time'; 'I had to explain to one of them yesterday the difference between the smugglers and the "boat people"'; 'Helpp! I don't like the idea of sending someone to jail' to which the lawyer asked, 'You're deliberating now?' and following the foreperson's response, 'Nahh, second accused is going through his case. But he's apparently hella poor, uneducated, family is barely eating sorta thing and I can't help but feel sorry for him :(' to which the lawyer replied, 'Dude you know you can't discuss anything about the case with people outside the jure. Stop.' 198-199.

(No 3).[1004] The social imperative that the accused be brought to trial, despite the unfairness of prejudice and pre-judgment outside the court's control was not considered by Nettle and Weinberg JJA to be relevant in considering whether the accused had a fair trial. If the trial was conducted 'with all the safeguards the law can provide, it was a trial according to law'[1005] the consideration that few cases had attracted greater pre-trial publicity in Victoria than this case known as the Faraday School kidnapping. However, after fifteen years of challenge to the jury system, Twitter can no longer be ignored. This new rapid, brief form of communication is leading many to consider that no matter what the safeguards, the time has come to question whether a jury trial can be remodelled or removed. The traditional methods for dealing with pre-trial publicity, such as changing the venue and delay orders have limited effectiveness because it is difficult to remove all access to social media and the internet. Sequestering the jury would be expensive and unwelcome.

Morrison considered that the internet with the wealth of information available, relatively effortless access, the capacity to blog, comment on social networks and generally solicit outside information, should lead us to rethink the role of the jury.[1006] The information sought by jurors has included researching details on Myspace about the profile of a victim in a sexual abuse case;[1007] accessing a defendant's Facebook page and viewing a photo of him with a gun;[1008] posting by a juror on his Facebook page the comment 'Stay tuned for the big announcement on Monday everyone!'[1009] posting on Facebook by a juror that the defendant was guilty before the defence case began;[1010] blogging by the foreman of a jury about the other jurors and details of the hearing[1011] and a juror who conducted a poll on Facebook because she couldn't decide if the accused was guilty or innocent.[1012] The shortcomings of current legal responses, such as jury instructions, confiscation of electronic devices, sequestration and fines were considered unworkable and at times, unenforceable.

[1004] *R v Dupas (No 3)* (2009) 28 VR 380 [253].
[1005] *R v Dupas (No 3)* (2009) 28 VR 380.
[1006] Caren Myers Morrison, 'Jury 2.0' (2010-2011) 62 *Hastings Law Journal* 1579-1632.
[1007] Ibid 1588.
[1008] Ibid.
[1009] Ibid 1600. This was during the corruption trial of a former Pennsylvania state senator Vincent Fumo – *United States v Fumo* No. 06-319, WL 1688482 at 61-62 (E.D. Pa. June 17, 2009).
[1010] Ibid 1601.
[1011] Ibid 1601 – *People v McNeely,* No. D048692, 2007 WL 1723711, at *2 (Cal. Ct. App. June 14, 2007).
[1012] Ibid 1602.

OSNs enable anyone to publish and such 'citizen journalists' are not as likely to be deterred by prosecution for sub judice contempt as professional journalists.[1013] It is also more challenging to prosecute social media users because it is difficult to determine what constitutes the prejudice. It is often the cumulative effect of tweets, posts and blogs.[1014] Social media has created a new dilemma for the use of non-publication orders [1015] and in some instances it has been shown to be futile to try to impose them because on the one hand they cannot be made in sufficiently extensive terms however to be effective against the global reach of social media, the orders needs to be wide.[1016] The issue is whether the courts are able to take control of the information disseminated.[1017]

Most OSN sites contain considerable personal information openly available. In *Strauss v Police*[1018] Justice Peek found that Facebook has become an investigative tool which allows users to search profiles, otherwise referred to as 'Facebook stalking' and has allowed a 'new generation of private investigators' to operate.[1019] The identifications made on Facebook were seen to contain none of the safeguards usually accompanying 'properly executed formal identification procedure conducted by the police'.[1020] Identifications from group photographs on Facebook were considered to be particularly dangerous by presenting 'a seductive and deceptive air of being a plausible identification' and by a 'displacement effect' will erase the subtle differences between the person identified and the offender. In this case the victim was given the name of the alleged offender and then a group photograph was located on Facebook in which the 'offender' was tagged.[1021] This was in circumstances where the alleged offender was drunk at the time of the assault and when he accessed Facebook was 'harbouring a visceral (and justified) grievance against his attacker'.[1022] His Honour also found a high degree of suggestibility in the identification by a witness who had accessed Facebook in the presence of another witness to the assault.[1023] His Honour considered that:

[1013] CCPIO Report, above n 882, 4.
[1014] Ibid 5.
[1015] These are orders which aim to prevent sub judice contempt before a trial.
[1016] CCPIO Report, above n 913, 7.
[1017] Pamela D Schulz, 'Trial by Tweet? Social media innovation or degradation? The future and challenge of change for courts' (2012) 22 *Journal of Judicial Administration* 29.
[1018] *Strauss v Police* (2013) SASR 90
[1019] *Strauss v Police* (2013) SASR 90, 103 [34].
[1020] *Strauss v Police* (2013) SASR 90, 103-104 [36]
[1021] *Strauss v Police* (2013) SASR 90, 104 [37].
[1022] *Strauss v Police* (2013) SASR 90, 104 [37].
[1023] *Strauss v Police* (2013) SASR 90. 133 [152].

> In the age of Facebook, the spectre of what is little more than speculation upon speculation very quickly solidifying into an "accepted view" is something that must be very closely guarded against when trying to bridge the chasm between social chit chat and proof beyond reasonable doubt in a court of law. [1024]

The substantial risk of contamination of evidence was of concern, particularly due to the collaboration of witnesses by 'simultaneous electronic communications' with an unlimited number of people in an unlimited number of physical locations exacerbating the problem.[1025]

Social networking sites have been held to present 'unique challenges for authentication' of evidence at trials.[1026] The evidence available on sites such as Facebook include individual profile pages (with details such as name, birthday, interests, current city and other identifying information), a variety of comments and links (these include photograph tagging which identifies people in a photograph and links to their profile page), private email messages and videos.[1027] An article by Griffith referred to concerns raised by US courts about people other than the owner of the site compromising accounts and posting unauthorized material. It has been held that a profile page is authentic if the information is so distinctive that it could only have been created by the person concerned. It was held on appeal in *Griffin v Maryland* that the information was not sufficiently distinctive on a MySpace profile produced in evidence at the trial. The authentication of evidence was of concern in *XY v Facebook Ireland Limited*[1028].

Because social networking sites contain such a 'fertile source of potential evidence' litigators should plan data collection methods which will ensure authentication so that important evidence in not excluded at trial. These websites were found to present unique challenges because they are 'cloud-based, transient, and collaborative in nature'. As Boehning and Toal found,[1029] social networks continue to play a significant role in federal and state court decision.

The credibility of OSNs as a source of information has been examined in relation to the how recently tweets were posted. It was found that the 'recency of tweets impacts source

[1024] *Strauss v Police* (2013) SASR 90, 102-103 [33].
[1025] *Strauss v Police* (2013) SASR 90, 102-103 [31]-[34].
[1026] Heather L Griffith, 'Understanding and Authenticating Evidence From Social Networking Sites' (2012) 7 *Washington Journal of Law and Technology* 209, 210.
[1027] Ibid 213.
[1028] *XY v Facebook Ireland Limited* [2012] NIQB 96 at [7]-[12].
[1029] H Christopher Boehning and Daniel J Toal, 'Authenticating Social Media Evidence' (2012) 248 (65) *New York Law Journal, Technology Today* <http://www.newyorklawjournal.com>.

credibility'[1030] and that this was an important 'as the gatekeeping function switches from producers to consumers of information for new technologies'.[1031] This issue is a relevant consideration for courts using OSNs and the issue of control of the information published. In most Twitter accounts the producer of the original tweet can lose control of the information as people accessing their comments add their own and change the dynamics of the message. They are no longer the gatekeepers of the information. This research indicates that there may be considerable danger in courts losing the 'gatekeeper' role because it may lead to unreliable information on their OSNs and therefore a loss of public confidence. The access to and control over information is constantly being negotiated in OSNs while the rules and norms shift with the needs of the users.[1032] A complex relationship has been identified between end users, third parties and the platform providers that is more complex in the era of big data.[1033]

Lawyer-client relationships can be created 'with a few clicks of the mouse' and non-lawyers can find themselves inadvertently and without authorisation practising law.[1034] It is this ethical issue that DiBianca considered. She warned of the problems lawyers face in complying with ethical responsibilities because the issues are 'many and complex and should be expected to change and develop with time'.[1035] It was considered important for all lawyers to familiarise themselves with the medium because 'ignoring social media altogether may constitute a violation of their ethical obligations'.[1036] DiBianca emphasised the duty of competence, the duty of diligence, the duty to preserve evidence and the duty of members of the American Bar Association to supervise lawyers in their use of social media. The duty of diligence owed by lawyers to their clients could also require detailed questioning of a client about their social media use to see whether the profile on sites such as Facebook contains information which could be 'potentially harmful' to the client.

It has been suggested that social networking has presented a minefield of ethical problems and complexity to the interaction between lawyers and their clients by impacting on issues such as

[1030] David Westerman et al, 'Social Media as Information Source: Recency of Updates and Credibility of Information' (2014) 19 *Journal of Computer-Mediated Communication* 171.
[1031] Ibid 172.
[1032] Cornelius Puschmann and Jean Burgess, 'The Politics of Twitter Data' Chapter 4 in Katrin Weller et al (eds) *Twitter and Society'* (Peter Lang, 2014).
[1033] Ibid.
[1034] Michael E Lackey Jr. and Joseph P. Minta 'Lawyers and Social Media: The Legal Ethics of Tweeting, Facebooking and Blogging' (2012) 28 *Touro Law Review* 149-182, 161.
[1035] Margaret M DiBianca 'Ethical Risks Arising from Lawyers' Use of (and Refusal to use) Social Media' (2011) 12 *Delaware Law Review* 179-198.
[1036] Ibid 180.

confidentiality, privileged communications, inadvertent disclosure and other aspects of the attorney-client relationship.[1037] Social media, blogs and any other interactive application that rely on cloud computing[1038] are at risk. When cloud computing is used, information is stored by a third party in another location which may be vulnerable to hacking. There may also be difficulties faced in rectifying the problems due to the complexity of international jurisdictions.[1039]

A lawyer's Facebook post was held to be relevant and discoverable in *Martin (Robert Gordon) and Heather Elaine Martin & Ors v Gabriele Giambrone P/A Giambrone & Law, Solicitors and European Lawyers.*[1040] The comment posted was:

> They thought they knocked me down, now they will see the full scale of my reaction. F*** them, just f*** them. They will be left with nothing.[1041]

The defendant solicitor claimed that the comments were confidential because only his friends could view them. However, Horner J held that the entry was relevant and discoverable, necessary for disposing fairly of the proceedings and that neither the solicitor nor the plaintiffs could have understood the information to be private and 'impressed with a "duty of confidence"'.[1042]

The concern of Lackey and Minta was the 'professional hazards' facing lawyers and the difficulties navigating the 'social media landscape' with professional rules prepared for an offline world.[1043] The common ethical problems discussed by Lackey and Minta were the duty of

[1037] Christina Vassilious Harvey, Mac R McDoy and Brook Sneath, '10 Tips for Avoiding Ethical Lapses When using Social Media' (January 2014) *Business Law Today,* American Bar Association, <https://www.americanbar.org/publications/blt/2014/01/03_harvey.html>.
[1038] Joe Kong, Xiaoxi Fan and K P Chow, 'Introduction to cloud computing and security issues, Chapter 1 in Anne S Y Cheung and Rolf H Weber (eds), *Privacy and Legal Issues in Cloud Computing* (Edward Elgar, 2015) 8—25.
[1039] Ibid 96-117.
[1040] *Martin (Robert Gordon) and Heather Elaine Martin & Ors v Gabriele Giambrone P/A Giambrone & Law, Solicitors and European Lawyers* [2013] NIQB 48.
[1041] *Martin (Robert Gordon) and Heather Elaine Martin & Ors v Gabriele Giambrone P/A Giambrone & Law, Solicitors and European Lawyers* [2013] NIQB 48.
[1042] *Martin (Robert Gordon) and Heather Elaine Martin & Ors v Gabriele Giambrone P/A Giambrone & Law, Solicitors and European Lawyers* [2013] NIQB 48, [12].
[1043] Michael E Lackey Jr. and Joseph P. Minta 'Lawyers and Social Media: The Legal Ethics of Tweeting, Facebooking and Bloggin' (2012) 28 *Touro Law Review* 149. Lackey and Minta in 2012 suggested that American lawyers cannot avoid social media because of the incredible amount of time a lot of people are spending on social media sites. By 2010 Americans were spending more than 20% of their online time on sites such as Facebook, Twitter and LinkedIn and even by 2009 more than 70% of lawyers were members of at least one sort of social

confidentiality, the limits on legal advertising and the unauthorized or inadvertent practice of law. As well, the dangers of posts on social media sites about judges and judicial proceedings and the specific problems facing judges and their employees who use social networks. The liability for legal advice offered online is another issue of concern particularly 'in a world increasingly being defined as cross-border cross-locality and cross-jurisdictional'.[1044] It is possible that social media creates further complexities for determining the vicarious liability of a legal practitioner where supervision of junior and non-legal staff already present considerable difficulty.[1045]

Judges, particularly in the US, have used OSNs to communicate with friends and colleagues. A District Court Judge in North Carolina was reprimanded for becoming 'friends'[1046] with an attorney on Facebook who was involved in a custody proceedings before the judge. They exchanged comments about the trial.[1047] In *Purvis v Commissioner of Social Security*[1048] the judge in considering the plaintiff's application for disability due to bronchial asthma, admitted that she had conducted her own research on Facebook and discovered a profile picture of the plaintiff where she appeared to be smoking. Few judges in Australia have been found to be using Twitter or Facebook for personal comments. A Judge of the Supreme Court of Victoria, Justice Lasry, described himself on Twitter as "Republican; Cyclist: Occasional Porsche racer; St Kilda FC follower …"and has 3,894 followers.[1049] In comparison, Justice Don Willett of the Texas Supreme Court has 64,400 followers. He is an elected judge and uses his Twitter account to connect with his voters. While judges may use their Twitter accounts with discretion, they cannot always control the OSNs of their family members. The daughter of Chief Justice Kourakis, Chloe Germanos-Kourakis, had to delete her Facebook post which criticised articles about barrister Claire O'Connor SC who had alleged sexual harassment by a District Court judge. Germanos-Kourakis claimed that the post was only intended to be read by her friends.[1050]

network.[1043] The Neilsen Social Media Report of 2012indicated that mobile applications accounted for more than a third of social networking time, although the computer remained the primary device for accessing social media.

[1044] Coralie Kenny and Tahlia Gordon, 'Social media issues for legal practice' (2012) 50(3) *Law Society Journal* 66-68, 68.

[1045] Ibid.

[1046] This is a term used on Facebook and other OSNs and which has a meaning specific to OSNs. It does not necessarily mean that there is a special relationship between people but implies a connection.

[1047] Emily M. Janoski-Haehlen, 'The Courts Are All A "Twitter": The Implications of Social Media Use in the Courts' 46 *Valparaiso University Law Review* 43-68, 57.

[1048] *Purvis v Commissioner of Social Security* No. 09-5318 (SDW) (MCA) 2011 (D.N.J. Feb. 23, 2011) 4.

[1049] Justice Lasry's Twitter account can be found with the identification @Lasry08 <https://twitter.com> .

[1050] The Facebook post by Germanos-Kourakis stated: 'I want to meet the sexist prick who wrote this article. The headline is insulting. It encompasses everything Claire was deploring. It mocks the sexual harassment both direct

The 'viral'[1051] spread of information over OSNs has been a cause of considerable concern, particularly in high profile criminal matters. The publication by the media of comments about victims and criminal offenders is not new, however, it has taken on a totally new dimension due to the inherent technological capabilities of interactive applications. This viral spread of information was demonstrated in the *Trafigura*[1052] case. There was a five week battle to keep the existence of the Minton report secret. [1053] This was exposed on Twitter and within 12 hours about a million people knew about the report.[1054] *The Guardian* wanted to publish the story about a Member of Parliament tabling a question in Parliament about the existence of an injunction but was prevented by the threat of contempt of court.

This difficulty faced by the legal system in controlling the spread of information and the interference by OSNs was demonstrated after the brutal death of Jill Meagher in 2012.[1055] There was also a claim of trial by social media with the comments on the Facebook page, 'Help us Find Jill Meagher'[1056] was created the following day when she had failed to return home. After the capture of the Adrian Bayley comments on OSNs reached a new level of intensity. Of concern to lawyers and the police were the comments inciting hatred and these were seen as undermining the legal system. The Attorney-General of Victoria warned Facebook to remove

and indirect we endure everyday. Sean Fewster you are a misogynistic dickhead', *Adelaide Advertiser* (5 November 2016) 'Off the Record'.

[1051] The adjective 'viral' was borrowed from scientific terminology and the theories of viral spread to marketing in the 1990s where is refers to the rapid spread of information, especially about a product or service amongst customers. As discussed by Sharad Goel et al, 'The Structural Virality of Online Diffusion' (2015) *Management Science,* Articles in Advance <http://dx.doi.org/10.1287/mnsc.2015.2158> "[w]hen a piece of online media content-say, a video, an image, or a news article-is said to have 'gone viral', it is generally understood not only to have rapidly become popular, but also to have attained its popularity through some process of person-to-person contagion, analogous to the spread of a biological virus". It 'implies a rapid, large-scale increase in adoption that is driven largely, if not exclusively, by peer-to-peer spreading". In this article the idea of structural virality was used to analyse a "unique data set of a billion diffusion events on Twitter, including the propagation of news stories, videos, images, and petitions".

[1052] *RJW & SJW v The Guardian newspaper & Person or Persons Unknown* (Claim no. HQ09)

[1053] This was a report commissioned in 2006 by Trafigura into an Ivory Coast toxic-dumping incident, protected by a super-injunction.

[1054] Staff reporter, *The Guardian* (16 October 2009) 'How the Trafigura story came to be told' <http://www.guardian.co.uk.>.

[1055] Gilliam 'Jill' Meagher, a 29 year old woman employed by the Australian Broadcasting Corporation, went missing about 2.00 am on Saturday 22 September 2012 and failed to return home after spending the night with work colleagues at bars in Melbourne. After four days there were 90,000 followers of the 'Help us Find Jill Meagher' web page and by 26 September there were about 800 comments including comments criticizing her behavior and the role her husband may have played in her disappearance. Her name hit almost 12 million Twitter news fees trending across Melbourne and Australia and her name was mentioned on Facebook and Twitter every 11 seconds. Adrian Ernest Bayle was found guilty of her rape and murder: *The Queen v Adrian Ernest Bayley* [2013] VSC 313.

[1056] Sanja Milivojevic and Alyce McGovern, 'The Death of Jill Meagher: Crime and Punishment on Social Media' (2014) 3 *International Journal for Crime, Justice and Social Democracy* 22, 23.

material that could jeopardise the trial or face legal action and they were removed the material by October 2012. A suppression order was made in the Melbourne Magistrates Court in an attempt to control the commentary on social networks which Deputy Chief Magistrate, Felicity Broughton, considered prejudicial.[1057] While the Deputy Chief Magistrate commented that most of the reporting had been in the mainstream media and 'the unregulated environment of internet sites might mean any ban was futile, the courts had a duty to try to protect the criminal justice process'.[1058] This difficulty of controlling such technology has been found to be an issue of concern. McGuire[1059] who considered that, 'technology has begun to acquire an increasing regulatory power of its own – operating as an autonomous force outside the realm of public scrutiny, accountability, or even control'.[1060]

Parties often claim that they are not responsible for posts on OSNs. The respondents in *Australian Competition and Consumer Commission v Allergy Pathway Pty Ltd* (No 2)[1061] were held by Finkelstein J to be liable for contempt of court because they knew that 'persons had published testimonials on its Twitter and Facebook pages and that it took no steps to have them removed'.[1062] Despite an undertaking provided to the Federal Court not to make, publish or cause to be made or published certain statements on its website relating to its testing and treatment methods for allergies.

Comments appearing on Facebook were claimed to be of a private nature in *Seafolly Pty Ltd v Madden*[1063]. This matter concerned misleading or deceptive conduct under s 52 of the *Trade Practices Act 1974* (Cth) in relation to swimwear designs where the respondent had published postings on her personal and company Facebook pages, particularly photographs of models wearing swimwear. It was stated by Justice Tracey stated that the application would need to establish that this conduct had occurred 'in trade and commerce'. His Honour held:

> In the present case, Ms Madden was the principal of White Sands, a trade competitor of Seafolly. Her statements related to the manner in which Seafolly conducted its business. She alleged that Seafolly had engaged in conduct which was improper to the detriment of

[1057] Mark Russell, 'Hate sites may affect Bayley's trial' *The Age* (10 October, 2012); Sarah Farnsworth, 'Court bans internet postings over Meagher case' *News ABC* (11 October 2012) <http://www.abc.net.au>
[1058] Sarah Farnsworth, 'Court bans internet postings over Meagher case' *News ABC* (11 October 2012) <http://www.abc.net.au>
[1059] M McGuire, *Technology, Crime and Justice: The Question Concerning Technomia* (Routledge, 2012).
[1060] Milivojevic and McGovern, above n 1056, 33.
[1061] *ACCC v Allergy Pathway (No 2)* (2011) 192 FCR 34.
[1062] *ACCC v Allergy Pathway (No 2)* (2011) 192 FCR 34, 42 [31].
[1063] *Seafolly Pty Ltd v Madden* (2012) 98 IPR 389.

> her own business. She thereby sought to influence the attitudes of customers and potential customers of Seafolly. In these circumstances, I consider that her statements were made "in trade or commerce".[1064]

There were also messages sent from the applicant's White Sands Facebook account to a personal Facebook account confidentially requesting the person to ask, 'Can you do me a massive favour, and ask me on facebook if a seafolly staff member DID pose as a buyer to photograph the collection. At least then I can get it out there in a legitimate forum!' A similar request was sent to another person to 'pose the question about Seafolly posing as buyers and photographing the collection'. The Full Court agreed with the primary judge about the public nature of the comments made and that there were statements that had 'a trading or commercial character'. The comments were considered in combination and it was found that it should not be concluded that any of the Facebook statements were 'of a private character.[1065]

The nature of posts by employees on OSNs have raised the issue of whether they are private or public. Generally in employment law, questions have arisen about the possibility of new obligations for employees and employers and questions concerning the vicarious liability of an employer for employees' social network postings.[1066] Potential liability for discrimination, defamation and infringement of intellectual property have also raised problems for users of social networks and challenges for lawyers as information is distributed rapidly, at low cost and on a monumental scale.

The liability for public postings of personal messages on Twitter message was considered in *Chambers v Director of Public Prosecutions*[1067]. In this case, when the Robin Hood Airport at Doncaster closed on 6 January 2010, the appellant posted the following message on his public timeline which could be read by about 600 people:

> Crap! Robin Hood Airport is closed. You've got a week and a bit to get your shit together otherwise I am blowing the airport sky high!![1068]

[1064] *Madden v Seafolly Pty Ltd* [2014] FCAFC 313 ALR 1, 24 [83] Rares and Robertson JJ.
[1065] *Madden v Seafolly Pty Ltd* [2014] FCAFC 313 ALR 1, 28 [98] Rares and Robertson JJ.
[1066] Elizabeth Raper, 'PokeMe:Rights and Responsibilities of Employers and Employees in the Age of Twitter, Facebook, YouTube and MySpace' (Paper presented at Sydney NSW Young Lawyers Seminar (10 June, 2009). See also Jennifer Farrell, 'Social Networking on company time: Can you control it?' (2011) 49 *Law Society Journal* 53-57 where the adoption of social media policies by companies was advocated to allow employers to use OSNs to improve communication while maintaining productivity and network security.
[1067] *Chambers v Director of Public Prosecutions* [2013] 1 All ER 149.
[1068] *Chambers v Director of Public Prosecutions* [2013] 1 All ER 149.

It was held by Lord Judge CJ, Owen and Griffith Williams JJ that on an objective assessment the message was not a 'message of menacing character'. Their Honours commented at that:

> Before concluding that a message is criminal on the basis that it represents a menace, its precise terms, and any inferences to be drawn from its precise terms, needs to be examined in the context in and the means by which the message was sent.[1069]

The context of *Chambers v Director of Public Prosecutions*[1070] was communication between friends on a public OSN and the expression of frustration that the airport would be closed and they would be unable to meet. The comment was meant as a joke with no intention that it would be considered menacing. This demonstrated that the exposure of spontaneous personal thoughts on OSNs by people which spread 'virally' can result in liability in the online environment not previously possible in the pre-digital era.

The application of existing law on a case-by-case basis was not considered to provide sufficient harmonisation or efficiency to 'meet the demands which social media are placing on them'.[1071] Scaife suggested that there is a need for a 'consolidated legal framework' to assist in determining the boundaries of freedom of expression and liability for infringement of other human rights. The changing role of the media largely initiated by developments in technology has highlighted the problem that 'it is not the media's role nor necessarily in the media's interest to necessarily provide the type and extent of coverage which the interests of the administration of justice appear to dictate'.[1072] The media is no longer the 'filter' for information. The concern is that with the challenge presented by Twitter which is able to present instant access to news stories that 'traditional media might focus more explicitly on the sensational elements of stories in an attempt to arrest the decline of the print and television medium'.[1073]

The minimalist nature of OSNs, particularly Twitter with its 140 character limitation, has been viewed as exacerbating the issue of increased scrutiny of the courts by enabling constant review and criticism, particularly with inaccuracy and a lack of objectivity. As Warren CJ referred to a criticism of the courts and the judiciary in relation to migration issues and people smuggling:

[1069] *Chambers v Director of Public Prosecutions* [2013] 1 All ER 149.
[1070] *Chambers v Director of Public Prosecutions* [2013] 1 All ER 149.
[1071] Laura Scaife, 'Tweet Revenge? Confusion on Social Media Limits' (2012) 23(3) *Computers & Law Magazine of SCL (Society for Computers and Law)* <http://www.scl.org>.
[1072] Daniel Stepniak, *Audio-Visual Coverage of Courts* (Cambridge University Press, 2008) 415.
[1073] Chief Justice Marilyn Warren, 'Open Justice in the Technological Age' (2013) 40 *Monash University Law Review* 45-58, 50.

> Sorry but we have the courts basically saying that anyone who rocks up to Australia can waste our courts [sic] time … Time to … get the courts out of the process … as our courts are making a mockery of the policy.[1074]

Controversial issues such as immigration, the appointment of former Chief Justice Tim Carmody in Queensland[1075] and the appointment of women judges in the United Kingdom by Lord Sumption have led to eruptions of instantaneous and emotional responses, particularly on Twitter. An English barrister, Dinah Rose QC led a Twitter attack on Lord Sumption following his claim that the '[r]ush for gender equality with top judges could have appalling consequences for justice':

> Here's what fascinates me: what does Lord Sumption think qualifies him to make these comments? Social scientist as well as a historian? (22 September 2015)[1076]

Before the advent of the new media, many courts had dedicated newspaper court reporters. The expertise of these reporters is being lost as court coverage has diminished and retired senior reporters have not been replaced. Few specialist legal reporters remain and it is unlikely that the citizen journalist on OSNs will 'be subject to any form of editorial control or commercial pressures, or bound by any ethical code'.[1077] Individuals publishing on OSNs have been viewed as 'essentially controllable only to the extent that their access to social media can be restricted'.[1078] The publication on new media is permanent, searchable and at times 'incrementally supplemented by interactive contributions – the author losing control over the tweet once published'.[1079] The mode of expression is often informal, sometimes offensive, inaccurate and lacking the 'customs and etiquette' of offline.[1080]

[1074] Ibid 52. Chief Justice Marilyn Warren quoting Jeremy Thompson, 'High Court Scuttles Malaysia Swap Deal', ABC News (online), 31 August 2011. <http://www.abc.net.au/news/2011-08-31/high-court-rules-on-asylum-seeker-challenge/2864218>.

[1075] On 1 July 2015, following the resignation of Tim Carmody as Chief Justice of Queensland, one tweet reported, "One time meatpacker, police officer, and chief justice Tim Carmody has fallen on his sword" <http://www.twitter.com>.

[1076] *UKSC blog* (22 September 2015) 'Rushing for gender equality' <http://ukscblog.com/rushing-for-gender-equality/>.

[1077] Jonathan Barrett, 'Open Justice or Open Season? Developments in Judicial Engagement with New Media' (2001) 11 *Queensland University of Technology Law and Justice Journal,* 1, 13.

[1078] Ibid 16.

[1079] Chief Justice Marilyn Warren, 'Open Justice in the Technological Age' (2014) 40 *Monash University Law Review* 45-58, 49.

[1080] Ibid.

The development of OSNs has changed the 'speed, range and duration of privacy intrusions'.[1081] They have eroded the balance between human rights, such as freedom of speech and privacy and questioned open access online, transforming transparency into overexposure. As former Chief Justice Spiegelman has stated in relation to an open mind, 'No doubt in most contexts an open mind must be regarded as a good thing. However, a mind that never shuts will generally be a public nuisance'.[1082] Open access on OSNs can be a public nuisance when transparency becomes overexposure of personal thoughts and data.

4.5 An experiment in using the opportunities offered by online social networks: The Supreme Court of Victoria

4.5.1 Introduction

In presenting the Redmond Barry Lecture in October 2013, the Hon Marilyn Warren, Chief Justice of Victoria, referred to the challenges 'driving the courts towards direct community engagement in order to preserve the operation of open justice'[1083]. Her Honour considered that '[t]he courts must develop constructive strategies to engage with the new technology if they are to guarantee open justice for all members of the community'.[1084] The courts can communicate more directly with the public and overcome the possible 'increased devaluation of the courts in the mind of the community'[1085] due to the traditional reticence of the judiciary to respond to criticism. Her Honour warned about the risks of the judiciary being 'trapped by its own traditions'[1086] and considered that it has become necessary for the courts 'to develop strategies of direct community engagement to preserve both open justice and public confidence in the judiciary'.[1087]

The Supreme Court of Victoria began using Twitter in 2011 and the use of Facebook in 2013. The Chief Justice considered that the development of 'new media' has changed the traditional methods of providing open justice for the public. Open justice no longer means open courtroom doors or using court reporters as the communication 'intermediary' but access via

[1081] Brownsword and Goodwin, above n 64, 236.
[1082] *McGovern v Ku-ring-gai Council* (2008) 72 NWLR 504-558,508.
[1083] Warren, above n 1074, 45.
[1084] Ibid 56.
[1085] Ibid 57.
[1086] Ibid 58.
[1087] Ibid 47.

the internet and social media which will provide the courts with the ability to communicate with a wider cross section of the community.

The recent transformation in court reporting and traditional journalism was considered to have challenged the court's traditional method of communication with the media and the public. The loss of 'the main source of dedicated and coherent media coverage of court proceedings' has meant that the courts need to reconsider 'who they should engage with and how they should engage in order to deliver a targeted and coherent message to the public' and so protect 'openness, public confidence in the judiciary and the right to a fair trial'. The balancing of open justice and the right to a fair trial was seen as a more difficult problem in the digital age.

Some of the strategies adopted by the Supreme Court of Victoria include the development of an interactive website which such features as: video on demand; judgment summaries and judgments available for downloading; the opportunity for the public to leave comments and participate in an internet forum; the publication of a regular blog by a retired judge and use of Twitter and Facebook.

The Supreme Court of Victoria uses social media, Twitter,[1088] Facebook and YouTube to share judgments handed down, media releases, new publications, speeches and administrative announcements. The Court has 'embraced new media technology to ensure a fundamental tenet of Australian democracy is fulfilled – that justice is not only done, but is also seen to be done'.[1089] It has been acknowledged internationally as one of the first Australian Courts to proactively use online social media.[1090]

4.5.2 Twitter analysis

4.5.2.1 Methodology

This analysis will present a quantitative and qualitative assessment of tweets by the Supreme Court of Victoria over two months (July and August 2015) to provide information about the way in which information is publicised, the degree of interaction and some indication of public interest in this method of communication with the court.

[1088] <http://www.twitter.com>. The Supreme Court of Victoria joined Twitter in February 2011 <https://twitter.com/SCVSupermeCourt>.
[1089] <http://www.supremecourt.vic.gov.au>.
[1090] Blackham and Williams, above n 848.

Previously a quantitative analysis was conducted by Blackham and Williams in 2014. The results indicated that many of the followers of the Victorian Supreme Court Twitter account were lawyers, journalists and university students which they considered perhaps reflected on 'the demographics on those who use Twitter in Australia'. The user profiles of followers revealed that close to 50% where based in Victoria. The authors concluded that while the use of Twitter had improved the Court's accessibility to a specialist audience it had not improved accessibility to the public at large. This may be attributed to the inherent conflict between the nature of courts and OSNs as referred to earlier in this chapter. The improved accessibility to the public may evolve as there is more routine use of OSNs by the courts and the public become more aware of this.

4.5.2.2 1 July to 31 August 2015

(a) Quantitative analysis

During this period there were over 40 Tweets by the Supreme Court. More than fifty percent of these related to information about seminars and tours available for the public as well as details about court procedures and filing. Information relating to the appointment and resignation of judges accounted for approximately 17% of the Tweets. These were accompanied by photographs. Just over thirty percent of the Tweets related to judgments and sentences handed down by the Court. These Tweets included a short statement with links to the decision or an audio file of the sentence, particularly for high profile criminal matters.

Table 1: Results of quantitative content analysis of types of tweets

Topic	**Frequency**	**Percentage**
Information • Seminars • Tours • Procedures	21	51.2%
Judgments	5	12.2%
Sentences	8	19.5%
Appointments	7	17.10%
Total	41	100%

Between 1 July and 31 August 2015 there were 41 Tweets which included a few Retweets[1091] from other parties. The most Tweets concerning information, whether details about tours of the Court, seminars or procedures such as links to the Practice Note 13 of 2015. References to judgments of the courts and sentencing together accounted for over 30% and about 17% of the Tweets referred to appointments or retirements of judges. This is only a small sample and future review may indicate a greater quantity of Tweets in the future and ones on different topics. This review does not indicate much about the details of the Tweets, their tone or content. The following is a brief qualitative analysis.

(b) Qualitative analysis

A review of the informational Tweets demonstrated information for the public about education tours such as one of the Supreme Court dungeons was most likely directed at school aged children:

> Jul 13 Dungeon tours at Supreme Court @OpenHouseMelb are fully booked, apologies to all who missed out, they book out within a matter of days.

Other educational events such as the Court of Appeal's 20th Anniversary public seminar was announced on Twitter:

> The video recording of the Court of Appeal's recent 20th anniversary public seminar http://ow.ly/RBXyu now available @JudicialCollege

The link is to the URL of the Judicial College of Victoria[1092] where there are three articles by judges are available and a video recording of the celebrations.

Judgments, particularly those that may be of public interest are available by link from the Supreme Court's Twitter site.

[1091] A retweet is a re-posting of someone else's Tweet which enables people to share information. Usually RT appears at the beginning of the Tweet to indicate that the comment is a retweet. There is also a Retweet icon and the name of the user who retweeted the comment.

[1092] The papers available on the Judicial College website are by: The Hon Justice Margaret McMurdo AC President, Queensland Court of Appeal, 'The advantages and disadvantages of permanent intermediate courts of appeal'; The Hon Justice Margaret Beazley AO, 'Judgment writing in intermediate and final courts of appeal' and by the Hon Justice Robert Redlich, Victorian Court of Appeal, '20th Anniversary of the Court of Appeal' <http://www.judicialcollege.vic.edu.au>.

> Aug 25 Justice Michael McDonald's judgment in the case involving Fertility Control Clinic v @cityofmelbourne now available, http://bit.ly/1LvRyzI

This refers to *Fertility Control Clinic v Melbourne City Council* [2015] VSC 424 handed down by the Supreme Court of Victoria on 26August. It was a matter of public interest because it involved a complaint by the Fertility Control Clinic to the Council about the conduct of protesters, associated with the Helpers of God's Precious Infants, over twenty years. The protesters had blocked the footpath outside the Clinic, approached women entering and leaving it and engaged in activities such as loud singing, praying and shouting which the Clinic found intimidating and harassing patients. It was held that the Council had directed itself to the question required, despite answering it incorrectly. The applicant was not entitled to mandamus.

Supreme Court of Vic retweeted

Shannon Deery @s_deery Aug 25

> @SCVSupremeCourt rules no failure by @cityofmelbourne by not stopping anti abortion protests. More @theheraldsun now pic.twitter.com/jxXd9SgiQX

The retweeting of this comment is some indication of the level of interest in the topic.

Details of sentencing are available from the Twitter account by way of a link to an audio file in a number of cases. The following is in a link to the audio file where Justice Terry Forrest sentences Isac Daing for the murder of his girlfriend. The file is accessed by a shortened Bitly[1093] link to the relevant uniform resource locator (URL). The webpage accessed has a photograph of Forrest J with a 25 minute 47 second audio file.

[1093] Bitly is a URL shortening service, established in New York City in 2008 which shortens approximately 600 million links per month, particularly for OSNs, such as Twitter with its 140 character limitation on Tweets, <https://bitly>.

> Aug 23 Listen to Justice Terry Forrest jail Isac Daing from Sudan for 18.6 yrs for murder of girlfriend, suffers PTSD, http://bit.ly/1NE9sCv

This was a high profile case considered of public interest due to the violent nature of the attack on Maryanne Sikai in which Daing was found to have beaten her 'to a pulp' with a kitchen stool. While Forrest J recognised Daing's traumatic life in Sudan and that Daing was suffering from posttraumatic stress, he found that '[t]here is a vital community interest in deterring powerful if inadequate males from terrorising their weaker female partners or ex-partners'. The case was widely reported in newspapers, particularly in Victoria[1094] as well as on Facebook and Twitter.

Information about appointment and retirement of judges are often accompanied by photos and videos. This can be demonstrated in the Tweet welcoming Justice Jan Dixon to the Supreme Court of Victoria.

> Aug 18 Welcome ceremony for Justice Jane Dixon to the Trial Division of the Supreme Court. pic.twitter.com/0VF3oBJp1I

The language used in the Tweets examples above is uniformly business-like and brief to conform to the 140 character limit, using abbreviations were possible. There is no use of colloquialisms or slang, although the language is simple and direct without complex legal terms. It can be contrasted with the tone of more commonly found on Twitter such as in the following one discussed in *McAlpine v Bercow*:[1095]

> Why is Lord McAlpine trending? *Innocent face*[1096]

[1094] Mark Russell, 'Isac Ayoul Daing jailed for beating girlfriend Maryanne Sidai to death with kitchen stool' (August 24, 2015) *The Age*: Wayne Flower, 'Isac Ayoul Daing jailed for the murder of Maryanne Sikai' (August 24, 2015) *Herald Sun*.
[1095] *McAlpine v Bercow* [2013] EWHC 1342.
[1096] *McAlpine v Bercow* [2013] EWHC 1342, [3].

It was held that this comment was meant 'in its natural and ordinary defamatory meaning, that the Claimant was a paedophile who was guilty of sexually abusing boys living in care' or the innuendo was to the same effect.[1097] The addition of the phrase 'innocent face' was claimed by the defendant to mean that she had noticed that there was interest in the topic on Twitter and she was asking people to tell her why. This was rejected by Justice Tugenhat who found that Bercow was being 'insincere and ironical'.[1098]

It gives some indication of the limitation that can be associated with providing comments and explanations in 140 characters. In this case the comments were understood by the judge in the context of the media reports.[1099] It illustrates the risk of tweeting and how easily words can be misunderstood yet widely published and the care that must be taken by courts using such a vehicle of communication.

4.5.2.3 Constructive strategies for OSNs

The Supreme Court of Victoria is actively using Twitter to communicate information about the Court, provide details about new procedures, judgments and sentencing to fulfil the aims of the Chief Justice to communicate directly to the public and preserve open justice. A review of the Supreme Court of Victoria Twitter account in August 2016 reveals the use has continued in a similar way with information about lectures, sentencing, appointment of judges and links to audio files.[1100]

The controlled manner in which such a popular OSN is used by this Court can be viewed as a constructive strategy to develop public confidence in the courts. The transparency presented is of the Court itself without inappropriate exposure of personal data relating to the cases, lawyers or judges. The Court has remained the gatekeeper of the information posted.

[1097] *McAlpine v Bercow* [2013] EWHC 1342 [90]-[91].

[1098] *McAlpine v Bercow* [2013] EWHC 1342 [84].

[1099] Sally Bercow, the wife of House of Commons Speaker in the UK, John Bercow. She published this Tweet shortly after the BBC Newsnight program broadcast a report on 2 November 2012 which included an allegation against a 'leading Conservative politician from the Thatcher years', without naming that person. This was widely reported in the media over the following days. The BBC apologized, however Sally Bercow did not admit that the Tweet was defamatory. Lord McAlpine brought proceedings for libel in relation to the publication of her Tweet to 56,000 of her followers.

[1100] Details can be viewed on the Supreme Court of Victoria Twitter pages <https:/twitter.com/SCVSupremeCourt>.

4.6 Conclusion

OSNs and the extraordinary numbers of people using them, whether lawyers, judges, non-lawyers, courts, government departments and business, have led to challenges not previously experience by the legal system, challenges related to both practice and procedure and substantive legal issues. They have opened a digital pathway in a transformed world of communication for the courts where the challenges have been described as 'widespread' with some activities 'evidently illegal, others border on legality, yet others are undesirable or morally indefensible'.[1101] Social networks have challenged the 'legal conceptions of privacy'[1102] and breaches of security and confidentiality have also been raised as serious concerns with the use of interactive technologies, particularly the risks associated with the compromise of client information.[1103]

This new online environment, 'where groups and individuals continuously and increasingly define themselves',[1104] is an environment that has the potential for courts to enhance access to justice, redefine their identity and improve communication with the public, thereby increasing confidence in the legal system. This can be achieved through a direct engagement by the courts themselves, not an engagement with the personnel of the courts and the judges and possibly an effective use of court media officers to monitor postings.

The courts need to ensure that the independence and integrity of the judiciary is strengthened rather than weakened by any overexposure of personal data and that they remain the gatekeeper for court information rather than allow rule by Facebook or any other OSN. At the same time, courts need to be conscious of the dangers of being trapped by tradition, using OSNs to improve communications with the public and reconciling the main contrasting characteristics between courts and OSNs.

In the following chapter I will examine the engagement of Australian Federal Courts in the digital enhancement of access to justice using Web 2.0 applications, a virtual courtroom, eCourtroom, which is used in the Federal Court and the Federal Circuit Court of Australia.

[1101] Carlisle George and Jackie Scerri, 'Web 2.0 and User-Generated Content: legal challenges in the new frontier' 2007) *Journal of Information, Law and Technology* <http://go.warwick.ac.uk/jilt/20072/george_scerri>
[1102] boyd and Ellison, above n 872. This article refers to the work of Hodge and the assertion that the fourth amendment to the US Constitution and legal decision about privacy which do not address social network sites.
[1103] Coralie Kenny and Tahlia Gordon, 'Social media issues for legal practice' (2012) 66 *Law Society Journal* 66, 68.
[1104] Floridi, above n 875.

Chapter Five – Virtual courts providing access and privacy: an empirical study of eCourtroom

5.1 Introduction

Virtual courtrooms are a dynamic method of justice delivery where access to justice is provided by the use of Web 2.0 applications, creating a digital pathway to justice. They have the capacity to enhance access to justice by providing improvements in efficiency, by creating savings in time and in the financial costs of litigation, as well as having the potential to improve transparency. In order to ascertain the role of virtual courts, in particular the use of eCourtroom, in enhancing access to justice in the Federal Court and Federal Circuit Court it is necessary to consider empirical data to complement the theoretical analysis. An understanding of this data will assist in ascertaining digital access and the role of personal information in the legal infosphere,[1105] facilitating an assessment of the tension between access and privacy in the electronic global environment. In this chapter I will discuss the theoretical basis for the use of virtual courts in providing access and open justice[1106] and will provide empirical data relating to the use of eCourtroom.

Two methods of qualitative analysis will be used to provide a more complete assessment of eCourtroom. The first analysis will consist of case studies of matters heard in eCourtroom to explain both the process and the outcome through observation and analysis at a micro level. This is a methodology suited to new research areas and can provide useful illustrations of the concepts discussed in this thesis. Case selection can be problematic, in that 'intrinsic to the concept is an element of doubt about the bias that may be contained in a sample of one or several',[1107] however, the issue of 'representativeness is not one that can ever be definitively settled in a case study'.[1108] As the variables are limited and the cases to be assessed relatively homogenous due to the limited variety of cases currently heard in eCourtroom, the probability is high that the cases selected are representative relative to the range of matters listed.[1109] This assessment will consist of an analysis of the public transcript of a representative selection of matters heard in 2014 that are available to the

[1105] Floridi, above n 561.
[1106] See Chapter Two, 'Access in the digital era', Chapter Three, 'Online exposure of personal information' and Chapter Four, 'Online social networks: enhancing access to justice?
[1107] John Gerring, *Case Study Research: Principles and Practices* (Cambridge University Press, 2007), 21.
[1108] Ibid 96.
[1109] See analysis of cases in eCourtroom 200-209 of this chapter. The categories of cases include applications for substituted service in Bankruptcy matters; Corporations examinations; and management of matters to be listed in Full Court appellate sittings at callovers.

public online, including a detailed content analysis of the applications, submissions and conduct of the matter electronically.[1110]

To add validity and reliability to the empirical research, the second methodology, qualitative content analysis, was chosen. It is research that can be distinguished from theoretical research by meeting specific information requirements with the potential for producing 'actionable outcomes'.[1111] It allows thematic analysis of data, producing summaries and synthesis while providing transparency and facilitating interpretation.[1112] The analysis consisted of an examination of responses to a questionnaire sent to Registrars of both the Federal Court and the Federal Circuit Court of Australia. The questionnaire contained five questions relating to the general experience of a virtual court, the advantages and disadvantages and possible privacy issues that might arise, despite the highly regulated environment.

The objective of the empirical research is to assess the enhancement of access to courts and the disclosure of personal information which is a necessary condition for participation in litigation where open justice is a priority. A fundamental issue is whether courts can control the online disclosure of personal data, particularly data linked to personal identity, viewed by Floridi as the weakest link[1113] in the protection of privacy, while using virtual courts. As 're-ontologizing technologies',[1114] virtual courts, have the potential to enhance or augment information privacy at the point of generation, the point of storage and the point of exploitation by self-regulation, legislation and technology.[1115] The complex issues associated with online disclosure of personal information will be considered and a number of policy options for the use of eCourtroom proposed. First, I will discuss the nature of virtual courts and the radical changes in access and dissemination of information they provide and second, the global digital environment in which they operate, before addressing the empirical research.

[1110] The electronic courtroom used in the Federal Court and Federal Circuit Court of Australia is referred to as eCourtroom (see explanation in Chapter 1 at 1.4) and details on the courts' websites at: <http://www.fedcourt.gov.au> and <http://www.federalcircuitcourt.gov.au> . It is a courtroom that exists only online.
[1111] Jane Ritchie and Liz Spencer, 'Qualitative Data Analysis for Applied Policy Research' in A Michael Huberman and Matthew B Miles (eds) *The Qualitative Researcher's Companion* (Sage Publications, 2002)
[1112] Aashish Srivastava and S Bruce Thomson, 'Framework Analysis: A Qualitative Methodology for Applied Policy Research' (2009) 4 *Journal of Administration & Governance* 72-79, 77.
[1113] Floridi, above n 561, 198.
[1114] Floridi, above n 561.
[1115] Ibid 190. Floridi refers to the protection of personal data (at the point of generation) by such technology as encryption; (at the point of storage) by legislation such as the provisions of the EU Data Protection Directive, 1995; and (at the point of exploitation) by technologies such as data-mining.

5.2 Virtual courts and the digital environment for eCourtroom

5.2.1 The virtual court

The nature of 'courts' can be seen to have changed in the digital era, particularly in relation to the method of access to court procedures and processes. While some features found in the pre-digital era have remained the same, there is less emphasis on the physical characteristics of authoritative, imposing court buildings and a transition in modern court buildings to light and openness, symbolising the transparency in the administration of justice.[1116] The more rigid time constraints and traditional hours have been replaced, particularly in virtual courts, such as eCourtroom, by a more adaptive process with a focus on efficient procedures.

Developing technologies have been used over the past twenty years to assist the courts to improve the efficiency and performance of court processes. These have mainly been sustaining technologies. In some Australian courts, electronic trials (eTrials) using electronic evidence which reduce the need for huge volumes of printed materials, have become more common, although the electronic materials have traditionally been managed by companies such as NuLegal[1117] and e.law[1118] in Australia, rather than by the courts themselves.[1119] In the US the use of videoconferencing in civil and criminal courts is not uncommon[1120]. In Singapore, Singapore Justice Online[1121] provides video conferencing, online document collaboration, court hearings and online meetings. A recent proposal in the UK was forecast to provide an online court system with evaluation, facilitation and pleading.[1122] What can be distinguished are those courts using technologies to increase efficiencies in the handling of documents and using audio-visual links to enable witnesses to present evidence

[1116] The new law courts of Caen, designed by BE Hauvette Paris and Atelier d'Architecture Pierre Champenois were described as providing the "message of transparency" from the design of the law courts and its extensive glazing (22 January 2013) <http://www.e-architect.co.uk/france/caen-law-courts>.

[1117] NuLegal website states that it exists "[t]o ensure that the quality and reliability of your legal expertise is supported by information technology and data management …" <http://www.nulegal.com.au>.

[1118] elaw website states that it is a about digital evidence, litigations support and legal technology service <http://elaw.com.au>.

[1119] The trial in *Seven Network Ltd v News Ltd* [2007] FCA 1062 (*'C7 Case'*) was conducted in an electronic courtroom and lasted for 120 hearing days. The electronic database contained 85,653 documents. The hearing was in a physical courtroom with the enormous database being managed electronically by the parties.

[1120] In *Bustillo v Hilliard* 16 Fed. Appx. 494, 2001 WL 894274 The appellant was require to participate in his civil trial by videoconference and remain in prison to minimize the chance that he might escape during the trial. Similarly in *Arrington v DaimlerChrysler Corp.* 109 Ohio St.ed 539, 2006-Ohio-3257 it was held that videotaped testimony did not offend the statutory right to trial by jury in claims pursuant to the Ohio workers' compensation statutory scheme.

[1121] Bizibody Technology is the leading provider of technology tools and web communications in Singapore. It provides court hearings in such matters as garnishee orders, probate and bankruptcy <http://justiceonline.com.sg>.

[1122] This new internet-based court service, HM Online Court would provide online dispute resolution for low value civil claims. It was recommended by the first report of the ODR Advisory Group of the Civil Justice Council (February 2015) <http://judiciary.gov.uk/reviews/online-dispute-resultion>.

from interstate or overseas, and those courts which do not have a physical presence but exist online and provide fundamentally different processes and procedures.

What can be distinguished is where technology is being used to assist traditional processes and where technology becomes a part of the process. A variety of terminology have been used to describe the different applications of technologies. Courts using developing technologies have been referred to as virtual courts, eCourts, courts with virtual services, cyber courts and more recently the expression 'distributed courts' has been used. The terms 'virtual courtroom', 'virtual services' and 'distributed court' all refer to various uses of technology in the courts.

The general term 'virtual courtroom' has been applied to courts whether using electronic court books and eTrials (electronic trials), electronic discovery where a significant part of the evidence is conveyed electronically, courtrooms using technology such as videoconferencing, computer simulation systems or simply those providing online tours of the physical facilities.[1123] The use of the term 'cyber court' was more common in the early days of virtual courts. It has been used, particularly in relation to the development of the Michigan cyber court system, the first virtual courthouse in 2002. At that time it was predicted that all proceedings would be conducted electronically with video and audio conferencing.[1124]

The term 'virtual services' has been also used to refer to a range of electronic and technological services provided by the courts. It can refer to 'any method to communicate other than face to face' or provide information other than in hard copy.[1125] Some of these are: remote interpreting to enable a greater availability of languages and to eliminate travel time, providing certified interpreters at any location; digital recording of hearings; remote appearances; video conferencing to avoid transporting parties in custody; e-filing and imaging of court records with solutions for self-represented litigants.[1126]

[1123] The Magistrates' Court of Victoria has a virtual court site which allows users to view mock court hearings and take part in an interactive virtual tour of a courtroom <http://multimedia.justice.vic.gov.au/egov/virtual_tour/magistrates-court-vic.html>.
[1124] Lucille M Ponte, 'Michigan Cyber Court: A Bold Experiment in the Development of the First Public Virtual Courthouse' (2002) 4 *North Carolina Journal of Law & Technology* 51-91. This cyber court built on the experiences of the Virtual Magistrate online dispute resolution experiment.
[1125] Susan Ledray, 'Virtual Services Whitepaper' *Harvard Journal of Law & Technology* (online) February 2013. <http://jolt.law.harvard.edu/symposium/articles/Ledray-VirtualServices.pdf> 1.
[1126] Ibid 2.

The use of the term 'distributed court', particularly for criminal cases, has been a more recent development where 'all the participants are thought of as being present in the same virtual three-dimensional space'.[1127] This development is still at an early stage. It has only been possible with the development of interactive technologies which allow a 'rich visual and acoustic stimuli' in a virtual environment where each participant joins the hearing from physical locations in courtrooms or court-like spaces created by 'immersive' video links.[1128] The aim of the distributed court is to represent a traditional, physical court in all aspects by creating an enhanced digital environment. In Australia, it has been based on the research of Tait[1129] and a research team in projects such as the *Gateways to Justice*[1130] which focussed on the design and operational guidelines for remote participation in court proceedings and on a more recent test of new procedures in a mock trial in May 2015.[1131]

What role technology will play in court procedures in the future will depend on many factors including; the sophistication of the technologies themselves; how adequate security for information can be provided; how appropriate particular technologies are for civil procedures or criminal matters; and to what extent they need to replicate the traditional courtroom by using 'immersive' technologies and life-like video links to provide the personal interaction expected in the traditional courtroom.

The development of virtual courts has been seen as increasing access to justice for low-income people by providing 'legal information and legal advice and for handling court business including hearings, interpreting, filing, and ancillary programs'.[1132] Research has focussed on the benefits of recent developments in technology[1133] and recognised that 'the place of technology in access to justice efforts has been cemented'. Ledray found that 'efficiency, costs savings, demands from the bar and public' as well as expectations that the technology of common use in business would be

[1127] Rick Sarre et al, 'Towards a Distributed Courtroom' (21 May 2015) Queen Elizabeth 11 Courts, Brisbane.
[1128] Ibid.
[1129] Multidisciplinary evidence-based research projects which examine the processes and rituals as well as physical and psychological setting of courts and tribunals, is conducted by the Justice Research Group, established in July 2009 at the Western Sydney University.
[1130] Emma Rowden et al, 'gateways to justice: *design and operational guidelines for remote participation in court proceedings'* (March 2013) <http://www.uws.edu.au/justice/justice/publiciations>.
[1131] Australasian Institute of Judicial Administration conference, *Justice Without Barriers: Technology for Greater Access to Justice* Brisbane.
[1132] Ledray, above n 1125, 2. 'virtual services' in a court setting were seen as including web-based self-help centers, remote interpreting, remote court reporting, phone and video conferencing for court hearings, payment of fines on-line, access to court records on-line, e-filing, classes via video conferencing and other services.
[1133] Ibid 3. The Pew Internet and American Life Project data (October 2011) reported that 64% of adults earning below $30,000 were using the internet and there was a high percentage of people using cell phones at all income levels.

available were pushing the adoption of technology in courts.[1134] As well, the cutbacks in budgets meant that courts needed to use technology 'to protect the public's access to courts'.[1135]

Bermant considered that 'the virtual courthouse is inevitable', however, the 'scope of the edifice and the design of its interior spaces' were negotiable.[1136] He considered that the use of technology 'relaxed the requirement of co-location' of trial participants in traditional spaces and the 'requirement of synchronicity' to enable the proceedings to be "'re-located" in both time and space'.[1137] Success in the application of innovative technologies, Bermant considered, was to be found in selecting proceedings that are sufficiently important and costly to warrant investment in improving their efficiency and effectiveness. Bermant found it quite reasonable to imagine technological procedures working for civil pre-trial proceedings, especially those involving discovery motions and bankruptcy proceedings, as can be found in eCourtroom.[1138]

In analysing the challenges facing state courts in the US, Scheb et al identified an intensifying movement towards 'virtual courts' and 'virtual interactions' as of significance for court governance, although they considered that the change was in the early stages of development.[1139] They distinguished the more radical view of Dator who considered it would become 'more and more rare for anyone to appear physically in any courtroom' as electronic communication brought 'the court to the place of controversy instead of the parties to the court'.[1140] Scheb et al explored the resistance to the use of virtual courts and found some authors preferred a hybrid system which would not replace all physical courtrooms but allow a digital pathway and a traditional pathway to operate together.[1141] A similar hybrid model was viewed by Kaplan as a way for 'courts to move forward while still maintaining tradition', the virtual courts providing additional access and economic benefits.[1142]. Not all case types were considered to be appropriate for virtual courts because, for some matters, the 'critical dynamic' provided to litigants when they enter a courtroom and the 'sense that justice is being dispensed because courthouses are symbols of justice', could be lost. [1143] In

[1134] Ibid 13.
[1135] Ibid 14. The 2009 National Center for State Courts Survey.
[1136] Gordon Bermant, 'Courting the Virtual: Federal Courts in an Age of Complete Inter-Connectedness' (1999) 25 *Ohio Northwestern University Law Review* 527-562, 528.
[1137] Ibid 549.
[1138] Ibid.
[1139] John M Scheb II et al, 'State Trial Courts: A Virtual Future?' (2012) 4 *Baker Center Journal of Applied Public* Policy 58-72.
[1140] Ibid 63.
[1141] Ibid 66.
[1142] Keith B Kaplan, 'Will virtual courts create courthouse relics?' (2013) 42 *Judges Journal* 32-36, 35.
[1143] Ibid.

assessing the future directions for courts in the technological era, Kaplan considered that courts needed to move forward while 'maintaining tradition'.[1144] Scheb et al recommended that this could be achieved by constant evaluation and research.

The virtual court, the focus of this empirical research, is one 'where the physical location of the courtroom does not dictate the process or the conduct of the proceedings' and where parties communicate 'over high-speed, high-quality electronic networks that permit interactive data, voice and visual transmissions'.[1145] These are courts that do not exist other than electronically.[1146]

5.2.2 The digital environment for virtual courts

A defining characteristic of the digital information era is its global quality, facilitated by Web 2.0 applications which enable courts to exist electronically. As Floridi has explained, '[w]e live in a single infosphere, which has no "outside" and where intra- and inter-community relations are more difficult to distinguish'.[1147] The employment of Web 2.0 applications in the delivery of services by the courts has implications for the control of personal data. It has relevance for the use of eCourtroom, which can be assessed in bankruptcy proceedings where extensive statutory disclosure provisions promote public access to information.[1148] This is a presumption that needs to be rebutted by the party seeking to overturn it. It is a presumption to be found in most common law countries.[1149] The legitimacy of the bankruptcy courts can be linked to the necessity for creditors, interested parties and the public to have sufficient information. This can be illustrated often by the

[1144] Ibid.

[1145] Anne Wallace, "'Virtual Justice in the Bush': The Use of Court Technology in Remote and Regional Australia' (2008) 19 *Journal of Law, Information and Science* 1-21, 6.

[1146] Gordon Bermant and Winton D Woods, 'Real Questions about the Virtual Courthouse' (1994) 78 *Judicature* 64-67, 64.

[1147] Floridi, above n 561, 193.

[1148] A number of sections of the *Bankruptcy Act 1966* (Cth) provide for disclosure by the bankrupt including: Section 265 of the *Bankruptcy Act* provides:

> (1) A bankrupt: (a) shall fully and truly disclose to the trustee all of the property of the bankrupt, and its value; (b) shall fully and truly disclose to the trustee particulars of any disposition of property made by him or her within the period of 2 years immediately preceding the date on which he or she became bankrupt; (c) shall not refuse or fail to comply with a direction by the trustee to deliver to the trustee property in the possession of the bankrupt, being all or part of the property of the bankrupt; …

Section 77(1)(f) of the *Bankruptcy Act* imposes an obligation on the bankrupt to "disclose to the trustee, as soon as practicable, property that is acquired by him or her, or devolves o him or her, before his or her discharge, being property divisible among his or her creditors".

[1149] In the US under Rule 2016 in a Chapter 9 or Chapter 11 case a disclosure statement under §1125 of the Code or evidence showing compliance with §1126(b) must be filed with the plan or within a time fixed by the court. In the UK the bankruptcy process is governed by the *Insolvency Act 1986* and the *Insolvency Rules 1986*. It is an offence for a bankrupt person to conceal a debt from the official receiver or trustee (Part IX, Chapter VI).

financial complexity created by bankrupts to hide assets from creditors particularly in overseas companies such as was found by the executors of the late Rene Rivkin.[1150]

It has been predicted that the issues of access to information and the control of that access will become more prevalent as documents and exhibits are filed electronically and made freely available on the internet for anyone with a computer to peruse at leisure.[1151] The permanence of this information on a global platform presents an inherent tension with the obligations of disclosure which is not intended to be lifelong.[1152]

The globalisation of financial transactions and mobility has created difficulties for the service of bankruptcy documents as well as creating new avenues for the service. The service of bankruptcy notices was traditionally only possible by personal service. Mason examined this issue in relation to such issues as the service of documents outside the Australian jurisdiction.[1153] Australian bankruptcy law has evolved to provide for a range of methods for service of documents, providing the creditor has evidence to support the contentions that 'in all reasonable probability, delivery to the address will be effective in bringing knowledge of the proceedings to the debtor'.[1154] Lawyers have been forced to think about bankruptcy notices in an entirely new way as people more recently have been engaged in 'concurrent media usage' and view several digital media outlets simultaneously, including online newspapers and blogs, email, social media sites and smartphone applications.[1155]

The use of 'modern modes of communication in this digital age'[1156] was seen by Kiel-Chisholm as being supported by the decisions in *American Express Australia Ltd v Michaels*[1157] where it was held

[1150] Susannah Moran, 'Rene Rivkin fortunes are lost forever' *The Australian* (Sydney) 16 April 2013. This article described the search in Australia, Jersey, London and Switzerland for millions of dollars missing from Rene Rivkin's $39 million bankrupt estate. His estate was placed into bankruptcy following his suicide in May 2005. The final dividend was about $3 million.

[1151] Mark D Bloom, David M Olenczuk and Richard L Wynne, 'Reorganizing in a Fish Bowl: Public Access vs. Protecting Confidential Information' (1999) 73 *American Bankruptcy Law Journal* 775-808, 776.

[1152] In *Re Todd; Ex parte Todd* (1986) 68 ALR 483, Pincus J held that the effect of provisions such as ss 43(2), 55(8) and 57(10) of the *Bankruptcy Act 1966* (Cth) was that the status of bankruptcy ceased with discharge so that the disclosure provisions cease with discharge; see *Madden v Official Trustee in Bankruptcy* [2014] FCA 446 where Farrell J discussed the implications of s 127 of the *Bankruptcy Act* as a limitation provision [42].

[1153] Rosalind Mason, 'Globalisation of Bankruptcy Practice – An Australian Perspective' (1997) 5 *Insolvency Law Journal* 12-23, 16 and 23.

[1154] Scott Kiel-Chisholm, 'Catch me if you can" the effective service of bankruptcy documents in a changing world' (201) 18 *Insolvency Law Journal* 197, 199.

[1155] Jeanne C Finegan, Craig E Johnson, 'New Media Creates New Expectations for Bankruptcy Notice Programs' (2011) *American Bankruptcy Institute Journal* 40; Leigh Adams, 'Clarity brought to service in cyberspace: electronic transactions laws fill the gap' (2010) 10(10) *Insolvency Law Bulletin* 168-169.

[1156] Kiel-Chisholm, above n 1154, 212.

[1157] *American Express Australia Ltd v Michaels* (2010) 237 FLR 268.

that documents could be served electronically to the defendant's email address and in *MKM Capital Pty Ltd v Corbo & Poyser*.[1158] Facebook was used for substituted service because the Facebook accounts could be conclusively linked to the bankrupt by date of birth and email addresses. At the commencement of insolvency processes, in the service of a bankruptcy notice or creditor's petition, the courts 'must balance the interests of the debtor, creditor and the community', especially with '[d]ebtors avoiding service, creditors using innovative ways to effect service and the court's interpretation of legislation'.[1159] This has been referred to as a 'dynamic environment of give and take'.[1160] Bankruptcy is also an area of law which illustrates the importance of open courts as well as the conflicting demands of privacy. The use of Web 2.0 applications and 'modern modes of communication' such as texting on mobile phones, Twitter, Facebook and skype, have particular relevance for bankruptcy documents, in providing effective service and resolving preliminary issues.

More than ten years ago Colby recognised a historical trend involving 'ever-widening concentric circles of human interaction, which necessitated a more elastic notion of personal jurisdiction in order to keep pace with commercial realities'.[1161] This 'prompted courts to adopt a corresponding flexibility with respect to service of process'.[1162] He predicted that electronic service would eventually become 'the rule rather than the exception'[1163] due to the expanded idea of personal jurisdiction and the increased 'inter-jurisdictional contacts among and between individuals and businesses'[1164] and the prevalence of the internet and email usage. No longer will 'process be nailed to a defendant's door when he can receive complete notice at an electronic terminal inside his very office'.[1165]

Paradoxically while the advancements in 'technology and travel have made evading service much easier than when society was considerably less mobile', technology has also presented a 'whole new world of possibilities for alternative methods of service of process'.[1166] This has been recognised as

[1158] *MKM Capital Pty Ltd v Corbo & Poyser* (Unreported, Supreme Court of the Australian Capital Territory, Master Harper, 12 December 2008).
[1159] Kiel-Chisholm, above n 1154, 211.
[1160] Ibid 198.
[1161] Jeremy A Colby, 'You've Got Mail: The Modern Trend Towards Universal Electronic Service of Process' (2003) 51 *Buffalo Law Review* 337-382, 381.
[1162] Ibid.
[1163] Ibid 338 and 380-382.
[1164] Ibid 345.
[1165] Ibid 354.
[1166] Keely Knapp, '#serviceofprocess@socialmedia: Accepting Social Media for Service of Process in the 21st Century' (2014) 74 *Louisiana Law Review* 547-579.

having an impact on Australian law.[1167] Bankruptcy notices can be sent by post, by email and via social media. The effectiveness of reg 16[1168] of the *Bankruptcy Regulations 1996* (Cth) was considered in *American Express Australia Ltd v Michaels.*[1169] In this case the court held that the use by Mr Michaels of his Yahoo email over the relevant period meant that he was 'maintaining' that facility and it came within reg 16.01(1)(e)(i) and that there were grounds for finding that electronic transmission of documents to his email address would be received by him 'in the ordinary course of events'. It appeared that Mr Michaels maintained places of business in Australia and possibly overseas. Section 14(6)(a) of the *Electronics Transactions Act* (Cth) was applied to deem his 'place of business' to be that which has a 'closer relationship to the underlying transaction' (his transactions with American Express) than the others and therefore the place of business was held to be Kent Street, Sydney which appeared on his application for credit from American Express.

Many debtors use evasion as a 'viable option' when facing financial difficulties which is reflected in the 'numerous applications made for the substituted service of bankruptcy notices and creditors' petitions'.[1170] By 2013 emails and OSNs were considered suitable for substituted service of documents in matters other than bankruptcy. In *Graves v West*[1171] the applicant had left Australia for the UK shortly after being convicted of recklessly causing grievous bodily harm. Judge Davies made an order for substituted service on the defendant by forwarding the documents via particular email and Linked-In 'In-Mail' addresses.[1172] Knapp has suggested that service through social media could be similar to service by mail. The message would be sent to the defendant's social media account with the petition and summons attached. She has suggested that there is more certainty and reliability in service via social media because on sites such as Facebook the sender can read the exact time the message is read by the recipient.[1173]

This flexibility which has been found useful for service of documents has been used in hearing bankruptcy matter in a virtual court. Such courts offer efficiencies not otherwise possible by

[1167] Kiel-Chisholm, above n 1154, 197.

[1168] Reg 16.01(1)(e) *Bankruptcy Regulations 1996* (Cth) provides that a document may be 'sent by facsimile transmission or another mode of electronic transmission: (i) to facility maintained by the person for receipt of electronically transmitted documents; or (ii) in such a manner (for example, by electronic mail) that the document should, in the ordinary course of events, be received by the person'.

[1169] *American Express Australia Ltd v Michaels* (2010) 237 *Federal Law Reports* 268.

[1170] Andrew Keay and Peter Kennedy, 'To Bankrupt, or Not to Bankrupt? The Question Faced by All Insolvency Advisers: Part One' (1993) 1 *Insolvency Law Journal* 187-198, 189.

[1171] *Graves v West* [2013] NSWSC 641.

[1172] *Graves v West (No 2)* [2015] NSWSC 306 at [7].

[1173] Knapp, above n 1166, 578.

offering online hearings which can be dealt with in an extended time frame,[1174] cost savings by allowing the matters to be dealt with from the practitioner's desk and saving the costs for parties travelling to court. It provides an open forum for communication as well as a controlled environment under the courts' direction.

Virtual courts such as eCourtroom and distributed courts which occupy a restricted environment at the same time sit in a global digital environment where the personal information necessarily available for litigation transactions can be subject to inadvertent disclosure at a number of points of collection. This can be caused by the failure of lawyers to redact personal information or administrative staff in the courts inadvertently disclosing information. This human error thereby making personal information widely available. This can be contrasted with the self and third party disclosure of OSNs.

The vulnerability of otherwise 'secure' data can be demonstrated by the evidence of numerous data breaches. The Data Breach event in February 2014 involved personal information relating to approximately 10,000 people who were in immigration detention and was inadvertently disclosed on the Department of Immigration and Border Protection's public website.[1175] In an amended application to the Federal Court of Australia, the applicant in *SZSSJ v Minister for Immigration and Border Protection*[1176] claimed that the Minister for Immigration and Border Protection had 'breached the applicant's privacy to information by releasing his name and other details on the departmental website'[1177] This breach of privacy of information, it was claimed, 'rendered the applicant a refugee *sur place*'[1178] under the UN Refugee Convention and failure to recognise that the applicant was a refugee *sur place* was a violation of procedural fairness. The applicant attached an abridged report of 20 May 2014 prepared by KPMG on the Data Breach.[1179] The application for an extension of time

[1174] Substituted service applications are listed before a Registrar in eCourtroom at a nominal time (4.00 pm) on the date listed in the filed application. As the examples discussed show at page [ ] these matters can be opened at a time that is convenient to the Registrar and the parties and the court may stay open for days or longer, if required.

[1175] *SZSSJ v Minister for Immigration and Border Protection* [2014] FCAFC 143; (2014) 231 FCR 285 [4].

[1176] Proceedings covered by S 91X of the *Migration Act 1958* (Cth) which provides for non-publication of applicants for a protection visa. A pseudonym protocol sets out the pseudonyms to be used in proceeding in the Federal Court and Federal Circuit Courts of Australia. The intention is that parties will have the same pseudonym in the all proceedings in the Federal Courts.

[1177] *SZSSJ v Minister for Immigration and Border Protection* [2014] FCAFC 143; (2014) 231 FCR [21].

[1178] This refers to people who may not fall within the definition of 'refugee' under the 1951 Convention Relating to the Status of Refugees because they may be held to have left their own country for non0refugee related reasons, however they may acquire a well-founded fear of persecution in their own country following their departure.

[1179] KPMG, Abridged report, 'Management initiated review: Privacy breach – Data management' <http://www.border.gov.au> This report found that the potential data access and distribution of a Microsoft Word document (dated 31 January 2014) Immigration Detention and Community Statistics Summary was widespread with 123 'hits' on the document from 104 unique IP addresses. It found that the personal information was not removed prior to

and leave to appeal was granted and the appeal was allowed. The matter was remitted to the Federal Circuit Court of Australia.[1180]

The OAIC received over 1600 privacy complaints from individuals affected by this data breach.[1181] The Commissioner found that the Department of Immigration and Border Protection had breached Information Privacy Principle (IPP) 4, 'by failing to put in place reasonable security safeguards to protect the personal information that it held against loss, unauthorised access, use, modification or disclosure and against other misuse'. [1182] The Department had also contravened IPP 11 by the unauthorised disclosure of the personal information when it was published. A further issue of concern was that the Detention report was available on The Internet Archive[1183] from 11 February 2014 until 27 February 2014 when the website complied with the request from the Department to remove the report. The Commissioner's report concluded:

> This data breach demonstrates the difficulties of effectively containing a breach where information has been published online, and highlights the importance of taking steps to minimise the risk of data breaches occurring, rather than relying on steps to attempt to contain them after they have occurred.[1184]

The Commissioner was particularly concerned about the disclosure because of the sensitivity of the data and the number of people involved in 'compiling, clearance and publication of the Detention report'. The reasonable security safeguard in this situation was held to be the de-identification of the information at an early stage of compilation.

---

the analysis being performed and the process adopted in producing and publishing this document did not confirm with the roles and responsibilities set out in the web publishing or the governance intranet guidance or online style guide. The factors found to have contributed to the incident may have been 'time pressures, unfamiliarity with certain functionality of Microsoft Word, lack of awareness of roles and responsibilities and limited awareness of IT security risks associated with online publishing'. The inadvertent access through the Department's website to the personal information was gained by 'a person/s unknown and passed to journalists/s at The Guardian'. The KPMG Report recommended specific measures, such as the development and implementation of procedure to normalise and clean any persona data extracted for analysis in a secure environment; updating of online publishing quality assurance checklists; IT security training programs; and holding publishing workshops, as well as general measures such as considering the current practices and procedures for the handling of sensitive data and the level of consultation with the IT security team in managing the risk.

[1180] *SZSSJ v Minister for Immigration and Border Protection* [2014] FCAFC 143; (2014) 231 FCR [37].

[1181] Media report: 12 November 2014 'Department of Immigration and Border Protection unlawfully disclosed personal information of asylum seekers', Office of the Australian Information Commissioner <https://www.oaic.gov.au>

[1182] *Department of Immigration and Border Protection: Own motion investigation report* (November 2014) <https://oaic.gov.au> IPPs – Information Privacy Principles (contained in s 14 of the *Privacy Act 1988* (Cth), prior to 12 March 2014.

[1183] The Internet Archive is a non-profit organisation founded in 1996 that builds an Internet library by archiving and preserving materials published on the internet, partly by an automated process which searches for and captures new publications. It has collected over 445 billion archived web pages.

[1184] *Department of Immigration and Border Protection: Own motion investigation report* (November 2014) <https://oaic.gov.au>.

Mr Nadir Sadiqi, a member of the minority Hazara group from Afghanistan and one of the applicants affected by the data breach, claimed that he received a death threat on Facebook from an alleged Taliban group that wrote that as soon as he returned to Afghanistan he would be beheaded.[1185] Mr Sadiqi deleted the message and closed his Facebook account. He sought intervention by the Minister after rejection of his claims.

The data breach issue has been raised as a ground of appeal and in many applications before the Federal Circuit Court[1186] and the Federal Court of Australia. In *SZUNZ v Minister for Immigration & Anor*[1187] the applicant raised the data breach issue before Judge Driver who found that it was not raised 'before the Tribunal (and apparently not before the delegate)'.[1188] The claim was based on the letter to the applicant from the Department attached to the applicant's affidavit, however it received no consideration by the delegate or the Tribunal.[1189] His Honour found that the applicant must show that the evidence raised considerations which must 'bear upon the material elements which must be satisfied, or rejected, when dealing with an applicant's claims'.[1190]

In *SZTKG v Minister for Immigration and Border Protection*[1191] while the data breach issue was raised by the appellant in ground 9 of the appeal, it was held that 'as indeed the Full Court considered in *SZTGV*[1192], that the data breach issue … is not directly raised in the circumstances … [and] because the data breach incident occurred after the Tribunal's decision and could not have figured in the decision making of the Tribunal' there was no jurisdictional error by the Tribunal.[1193] In *SZTYO*[1194] the data breach issue was also raised in an application for an interlocutory injunction to restrain the Minister for transferring the applicant from Villawood Immigration Detention Centre to the Wickham Point Immigration Detention Centre. The applicant's solicitor submitted that she would not be able to attend the International Treaties Obligations Assessment interview with the applicant

[1185] Nicole Hasham, 'Asylum-seeker victim of government privacy breach fears being murdered by Taliban' (11 July7 2015).
[1186] Cases in 2014 include: *SZSSJ v Minister for Immigration & Anor* [2014] FCCA 1379 (20 June 2014); *SZULJ v Minister for Immigration & Anor* [2014] FCCA 2611 (14 November 2014); and in 2015, *AAW15 v Minister for Immigration & Anor* [2015] FCCA 643; *MZADZ v Minister for Immigration & Anor* [2015] FCCA 1589 (18 June 2015); *SZVUM v Minister for Immigration & Anor* [2015] FCCA 2263 (21 August 2015).
[1187] *SZUNZ v Minister for Immigration & Anor* [2014] FCCA 2256 (17 October 2014).
[1188] *SZUNZ v Minister for Immigration & Anor* [2014] FCCA 2256 (17 October 2014) [30]-[31].
[1189] *SZUNZ v Minister for Immigration & Anor* [2014] FCCA 2256 (17 October 2014) [29]-[30].
[1190] Judge Driver referred to the decision of Robertson J in *Minister for Immigration and Citizenship v SZRKT* (2013) FCR 99, 132 [121].
[1191] *SZTKG v Minister for Immigration and Border Protection* [2015] FCA 267 [21].
[1192] *SZTGV v Minister for Immigration and Border Protection* [2015] FCAFC 3 [2].
[1193] *SZTKG v Minister for Immigration and Border Protection* [2015] FCA 267 [22].
[1194] *SZTYO v Minister for Immigration and Border Protection* [2015] FCA 30.

when the Department assessed whether, 'as a result of the 2014 data breach, Australia's *non-refoulement* obligations had not been complied with'.[1195] It was held that the applicant failed to establish that there was a serious question to be tried and as the interlocutory injunction does not finally determine any rights he might have and is 'in aid of private rights', the injunction was refused.

Whether such problems have been caused by human error or the use of vulnerable security systems or any other issue, once such information is released the regulatory challenge of providing a 'right to be forgotten' and a 'right to erasure' remains, as can be currently seen in the burden faced by Google to remove links disclosing personal information.[1196]

Security issues remain of ongoing concern not only for individuals but for businesses and government departments, as indicated by the security breaches reported in 2016.[1197] A detailed discussion of such issues is not within the scope of this thesis, however, the extent of the threat to computer systems indicates that the protection of personal data and identity theft will remain an issue of concern for the future and dictate prudence in the adoption of Web 2.0 applications by the courts as well as measures to provide some degree of the practical obscurity provided in the past by hard copy record.

5.3 Regulating eCourtroom for privacy

The Federal Court and Federal Circuit Courts of Australia have detailed policies for the protection of privacy and security of personal information on eCourtroom. This is supported by the *Privacy Act 1988* (Cth) in relation to an act done or a practice engaged in in respect of a matter of an administrative nature, however court documents are exempt[1198] from the *Privacy Act*. The Courts are committed to protect privacy and adhere to the *Guidelines for Federal and ACT Government Websites*[1199] developed by the Privacy Commissioner.

[1195] *SZTYO v Minister for Immigration and Border Protection* [2015] FCA 30 [37].

[1196] Google Transparency Report This transparency report is published twice a year. From May 29, 2014 Google has evaluated 1,235,473 URLs for removal from 348,508 requests <http://www.google.com/transparencyreport/removals/europeprivacy/>.

[1197] Ian Paul, 'The 10 biggest hacks, breaches, and security stories of 2016' (21 December 2016) *PCWorld* (online) <http://www.pcworld.com>. Paul reported that 'Yahoo broke the record for allowing the largest hack in history' when approximately 500 million user accounts were breached; ramsomware, malware that encrypts computer files and holds them hostage or deletes them, was used prolifically during 2016, 'hitting half of all U.S. businesses'. It was also reported that 'computer hacking graduated from harassing businesses and government agencies to direct intervention in the U.S. presidential election' when the computer network of the Democratic National Committee' was hacked.

[1198] Section 7(1)(a) and (b) of the *Privacy Act 1988* (Cth).

[1199] Privacy Guidelines <https://www.oaic.gov.au/agencies-and-organisations/guides/>.

The Federal Court of Australia Privacy Policy[1200] lists the information that is recorded when personal information is provided for participation in eCourtroom.[1201] It includes data needed for troubleshooting, major and specific activity under a user name. There is an assurance that email address information is only used for the purpose for which users provide it. When personal information is stored in paper files and password protected electronic databases. Specific provisions have been made for electronic court files by Practice Note *CM* 23 particularly in relation to the elimination or protection of personal and sensitive information.[1202] Court proceedings in the Federal Court, the Federal Circuit Court are exempt from the *Privacy Act* except for acts done or a practice in relation to the management and administration of the registry and office resources. In addition to this the Court recognises the sensitivity of personal information and states that it will 'make arrangements that are consistent with all legal requirements and which balance appropriately the principle of open justice and interests of individual privacy'. Reference is made to the Court's privacy policy[1203] and the Guidelines for Federal and ACT Government Websites.[1204] The changes

[1200] The Federal Court of Australia Privacy Policy is available at <http://www.fedcourt.gov.au/privacy/full-privacy-policy>.

[1201] Other information recorded includes the uploaded documents and failed attempts to upload documents which are logged in error logs; cookies are used for authentication and browser preferences for display of results. E-commerce industry standard security communications protocol (HTTPS) is used with upt o 256 bit encryption to ensure all data transmitted between the user's computer and the Federal Court's eLodgment Web Portal is secure.

[1202] Practice Note CM 2, 'Electronic Court File and preparation and lodgment of documents' (10 July 2014) 6.4 provides: 'Unless this is restricted by a suppression or non-publication order or statute, a document which is accepted for filing may be inspected and copied by any person either with or without leave depending on its nature. To limit possible infringement of individual privacy, the risk of identity theft and frequent applications for suppression and non-publication orders, every effort should be made to eliminate from documents all unnecessary personal or sensitive information about any individual. In particular, unique personal identifiers, such as past or present residential addresses, dates of birth, anniversary dates, telephone numbers, email addresses, vehicle registration, passport numbers, Medicare numbers, bank or financial institution account numbers of all types, other financial dealing numbers of all types, Tax File Numbers, vehicle licence numbers, Centrelink reference numbers and employee or enrolment identification numbers of all types, should either be omitted or a substitution used. For example it may be sufficient to use the year rather than the date of birth. It may be sufficient to obscure all but the final few digits of unique personal numbers' <http://www.fedcourt.gov.au>.

[1203] Privacy Policy at <http://www.fedcourt.gov.au/privacy/full-privacy-policy>.

[1204] These guidelines were developed in 2003 <http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guidelines-for-federal-and-act-government-websites#1> to assist government agencies to adopt best privacy practice and comply with the *Privacy Act 1988* (Cth), particularly with respect to the personal information that may be "transmitted, published, solicited and collected via the internet" on their websites. The guidelines provides reference to the Office of the Australian Information Commissioner (OAIC) for further advice and updates on privacy policies. The background concerns related to the lack of transparency in the use and disclosure of personal information, tracking of individual's activities and the security of personal information in the internet environment. Guideline 1 provides that "Agency websites should incorporate a prominently displayed Privacy Statement which states what information is collected, for what purpose and how this information is used, if it is disclosed and to whom and addresses any other relevant privacy issues; Guideline 2 provides, Agencies that solicitors who collect personal information via their website must comply with IPPs 1 – 3. Agency website privacy statements should include a statement regarding this collection which complies with IPP 2. Where an online form is used to collect personal information the statement should be on the same page as the form or prominently linked to it. Guideline 3 provides, if personal information is collected via an agency website this should be done by sufficiently secure means, Individuals should be provided with alternative means of providing personal information to the agency, other than via the website. The Privacy statement should address security issues where appropriate. There is a note that the guidelines may not reflect the current law, particularly since the changes to the *Privacy* Act in March 2015. Users are to refer to The Web Publishing Guide

in privacy policy and guidelines for government agencies reflects the considerable changes in privacy law, in the *Privacy Act* and the attempts by law to keep up with technological change.

The rules for using eCourtroom are set out in the Federal Court Protocol[1205] which supplements the provisions of the *Privacy Act* and government guidelines for privacy and websites. It states that using this virtual courtroom 'is the equivalent of conducting a matter in an ordinary courtroom' because it is to be used only for consideration of issues and determination by the Court or a judge, not for communication between parties or their representatives, particularly not for sensitive or confidential information. The language and mode of address is to be the same as in an ordinary courtroom, the rules of contempt apply and undertakings given by a party or their representatives will be binding as if given in an ordinary courtroom. Notification is also given that the 'discussion thread' will be publically available as read-only text on the Court's web site.

The Protocol specifies that the Court or a judge will decide what matters will be dealt with, when the matter will be terminated and, where required, give directions on matters such as the topics, who can participate, the length of messages and the maximum time in which the messages can be sent. There are provisions for the filing of documents, consent orders and the possible use for mediations. Each party or participant is given their own account name and password which are to be kept confidential and secure. As a further security safeguard, it is provided that '[t]he Court or a Judge will deem that messages and documents sent to the eCourtroom from a particular account have been sent by, and are the responsibility of, the person to whom that account was allocated'. This provision provides some protection for the Court if the person's account is used by someone else, with or without their knowledge.

The personal information on eCourtroom is relatively secure in the context of Bankruptcy Law which promotes openness and public access to information. The public transcript information is only available to those with internet access and knowledge that it exists. What is not clear is the extent to which information can be redacted and protected for the discharged bankrupt, particularly considering the permanency of information on the internet compared to the practical obscurity of paper records. It is the reintroduction of practical obscurity to the digital era that the 'right to be

(<http://webpublishing.agimo.gov.au>). This site is no longer available. From 1 July 2015 the Digital Transformation Office (DTO) <https://www.dto.gov.au> will be responsible for whole-of-government web guidance and the Web Guide will be superseded by the Digital Service Standard and Digital Service Design <http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guidelines-for-federal-and-act-government-websites#1>.

[1205] Federal Court of Australia eCourtroom Protocol: <http://www.fedcourt.gov.au/online-services/ecourtroom/protocol>.

forgotten', discussed in the following chapter, has the potential to achieve by enabling a deliberate disconnect for digital data.

If skype-like facilities are added to eCourtroom to enable computer linked facilities for examinations of the bankrupt or 'examinable person'[1206] in relation to the property of the bankrupt there may be additional security risks. It has been suggested that using such facilities would improve access to justice 'because parties could have easier access to lawyers'.[1207] It would also save costs and allow lawyers to appear in several courts in different locations in one day.[1208] Krawitz and Howard considered the use of VoIP[1209] to have security issues because its use can open proceedings to a less secure environment than videoconferencing and the use of a dedicated ISDN line.[1210] They found that Skype had had limited use in courtrooms in Australia and overseas, however, they did not consider that Skype was unsuitable for the court environment and potentially future use could facilitate access to justice.[1211]

In cases where Skype has been used, following consideration of the administration of justice and the exercise of discretion, that it is technology that can provide a solution to difficult circumstances. In *Rezaeipoor v Arabhalvai*[1212] in the UK Deputy Judge Kevin Prosser QC upheld the Master's discretion to allow the case management decision to allow the use of Skype for cross-examination of a witness in Iran. In this case the witness had done everything possible to obtain a visa to enter the UK but it had been refused. There were no private video conferencing facilities in Iran and the Master was concerned about the uncertainty that a visa would be granted even if a substantial adjournment had been granted. The Master considered any possible prejudice to the applicant by the use of Skype

[1206] Section 81 of the *Bankruptcy Act 1966* (Cth) contains detailed provisions for examination "(1) Where a person … becomes a bankrupt, the Court or a Registrar may at any time (whether before or after the end of the bankruptcy), on the application of: (a) a person (in this section called a ***creditor***) who has or had a debt provable in the bankruptcy; (b) the trustee of the relevant person's estate; or c) the Official Receiver; summon the relevant person, or an examinable person in relation to the relevant person, for examination in relation to the bankruptcy … "

[1207] Marilyn Krawitz and Justine Howard, 'Should Australian courts give more witnesses the right to Skype? (2015) 25 *Journal of Judicial Administration* 44-63, 63.

[1208] Ibid.

[1209] VoIP is Voice over Internet Protocol, a group of technologies which deliver voice and multimedia session of IP networks. They can be open or closed networks for private or public use.

[1210] ISDN is an Integrated Services for Digital Network which provides a set of communication standards for digital transmission over traditional telephone networks, integrating speech and data.

[1211] Krawitz and Howard, above n 1207, 57. They referred to the comments of Jackson J in *Re ML (Use of Skype Technology)* [2013] EWHC 2091 (Fam) concerning the use of Skype. His Honour considered Skype more appropriate for informal use but a technology that could present issues of security, and problems with the recording of evidence as well as visual and auditory clarity for a court hearing. The problem was resolved in this case by Eyenetwork a company specializing in video conferencing and video bridging because it was able to provide some protection from hacking. The judge appreciated the cost and time savings in using this company's system rather than an ISDN. It was found to be of particular use for remote locations where there were few option for video conference facilities, such as Colombia and remote areas of Nepal.

[1212] *Rezaeipoor v Arbhalvai* [2012] EWHC 146 (Ch).

and agreed that 'an imperfect solution' was to be preferred for 'the efficient, fair and economic disposal of the case'. On appeal Prosser J held that the Master had been justified in permitting the use of Skype.

I will now analyse, in detail, the use of eCourtroom as a virtual court and discuss the issues relating to the enhancement of access to justice.

5.4 The Use of eCourtroom – an empirical analysis.

5.4.1 Transition to a virtual process

Applications for the substituted service of bankruptcy notices and creditors' petitions are common in the Federal Courts.[1213] Until the introduction of eCourtroom these matters were listed in a physical courtroom.

When first used, eCourtroom was a stand-alone application and was not integrated with the case management system,[1214] eLodgment[1215] and the Commonwealth Courts Portal.[1216] At first referred to as the eCourt Forum it began operating in 2001 using a secure 'bulletin board' where messages and documents relating to a particular case could be posted. It enabled interlocutory matters 'to be discussed, reviewed and orders made by Internet-based dialogue between counsel, law firms and the judge'.[1217] It was used in native title cases where it was found to be 'very effective in keeping large numbers of widely dispersed parties in touch with the progress of the litigation'.[1218]

The Charter of the Federal Court as stated by the Principal Registrar was to 'integrate our eCourt Systems in order to fully realise the potential of technology to enhance services, and to improve access to justice for the wider community'.[1219] The integration was implemented in 2007 with the

[1213] The Federal Court of Australia and the Federal Circuit Court have concurrent jurisdiction in Bankruptcy. In 2014-2015 41/3% of matters filed in the Federal Circuit Court were bankruptcy matters <www.federalcircuitcourt.gov.au> Annual Report 2014-2015.

[1214] <http://www.fedcourt.gov.au> Casetrack is the case management system used by the Federal Court and Federal Circuit Court.

[1215] <http://www.fedcourt.gov.au>.

[1216] <https://www.comcourts.gov.au> The Commonwealth Courts Portal provides web-based services to enable litigants and legal practitioners to enable them to access information about cases before the courts. It is an initiative of the Family Court of Australia, the Federal Court of Australia and the Federal Circuit Court of Australia. By using the Federal Law Search on this site it is possible to access selected information about cases.

[1217] Michael E J Black, Chief Justice of the Federal Court of Australia, 'New Technology Developments in the Courts: Usages, Trends and Recent Developments in Australia', a paper presented at the Seventh Worldwide Common Law Judiciary Conference, (May 2007) 21.

[1218] Ibid.

[1219] Jo Sherman and Allison Stanfield, 'Federal Court of Australia: eCourt Integration Strategy Final Report' (January 2004) 18 <http://*www.aph.gov.au/~/media/Estimates/Live/legcon_ctte/estimates/bud.../155_att.ashx*> .

aim of ensuring all the information relating to a file, including orders, party contact details and listings would be available from 'one comprehensive and intuitive environment'.[1220] The interactive virtual courtroom continued to form an integral part of eCourt services with the on-line forum being renamed eCourtroom. The plan was to use an email system specific to eCourtroom which would differ from normal email by automatically linking each message to the relevant Casetrack file.[1221] It provides a superior system for capturing the flow of comments and responses between the parties. It was considered to be more cost efficient because it avoids duplication. The system uses a central storage location and also provides brief email alerts with links to the message in the central system rather than to the email containing the message itself.

In both the Federal Court and the Federal Circuit Court of Australia, the eCourtroom is used to manage and hear pre-trial matters such as ex parte applications for substituted service in bankruptcy proceedings and applications for examination summonses. It is a virtual courtroom in that it does not exist physically. Technology is used as more than a tool for facilitating the hearing, as in an eTrial, but the Web 2.0 applications become a part of the process. It has been found to be more suitable for less complex interlocutory matters and case management hearings. The protocols are the same as those used in a physical courtroom and the transcript can be viewed by the public online. A matter is placed on eCourtroom at the direction of a judge or registrar. The administrator sets up the participants on the system with user ID and passwords assigned to them. The parties are notified by email. Physical attendance at the Court is not required. This provides parties with additional time to give considered responses and can save costs, particularly in bankruptcy proceedings. Orders are made online.

The most common listing in eCourtroom is an application for substituted service. All matters in the Federal Court and Federal Circuit Court of Australia may be commenced by electronic lodgement. Practice Note CM 20[1222] in the Federal Court states that eCourtroom is 'a virtual courtroom that assists in the management of pre-trial matters by allowing directions and other orders to be made

[1220] Ibid. Because many of the functions and activities of the Court's external clients were found to be identical to those of the internal staff, it was planned to use consistent software application interfaces for both internal and external users. This would lead to easy use, minimise costs, enable judges to use the same interface in chambers or from a remote location, allow maximum regional access, reduce duplication, and provide the certain access to judges which would not be available to litigants or lawyers.

[1221] Casetrack is the case management system used by the Federal Court, the Family Court and the Federal Circuit Court of Australia <http://www.fedcourt.gov.au>.

[1222] Practice Note CM 20, 'Ex parte applications for substituted service in bankruptcy proceedings and applications for examination summonses under section 81 *Bankruptcy Act 1966* and sections 596A and 596B *Corporations Act 2001*' was issued 3 September 2014 It outlines the procedures to be followed for registering for eCourtroom and explains how practitioners sign up for a particular matter, <http://www.fedcourt.gov.au>.

online'. It provides that all new applications for orders for substituted service of bankruptcy notices or creditor's petitions; for the issue of examination summonses under s 81 *Bankruptcy Act 1966* (Cth); ss 596A and 596B *Corporations Act 2001* (Cth) are usually dealt with by hearings in eCourtroom. Litigants may file the documents by electronic lodgement through the eLodgment portal. The practitioners must provide their full name and email address on the application. An email notification is sent to the practitioners with a return date and eCourtroom as the location of the hearing. Before this date the Registrar will communicate with the practitioner via eCase Administration. This is used for the filing of evidence and the submission of draft orders, which must be sent in Microsoft Word format. The matters are to be considered within ten business days of filing and the hearing in eCourtroom on the date listed on the application. The process allows for flexibility in listings which is referred to in the following section of this chapter.

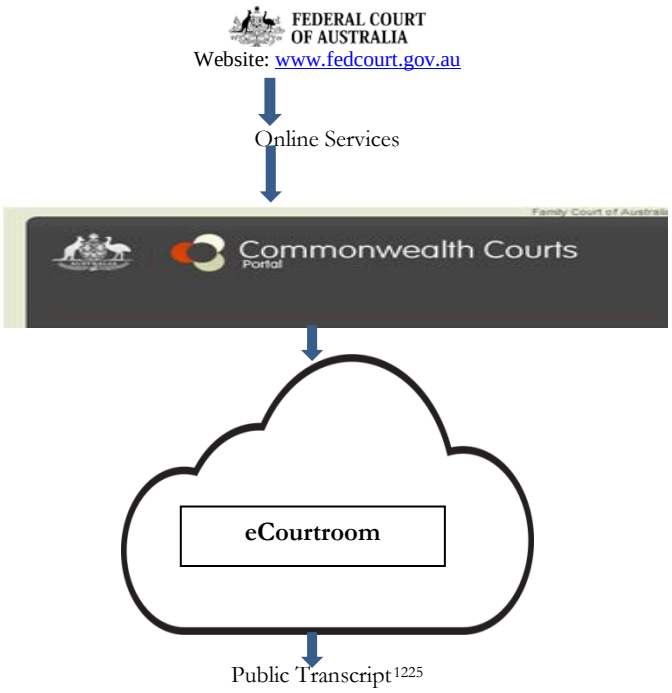
Other uses for eCourtroom are for Full Court callovers when the status of matters to be listed in the quarterly Full Court sittings are assessed.[1223] This has become routine in the Federal Court since 2005. The parties are notified of the callover date approximately three weeks beforehand and also receive a Full Court Status Report for completions by email. The Deputy District Registrar (DDR, also referred to as Registrar) opens the hearing on eCourtroom and during this time the parties can advise the Judge of any additional information will need to be considered. The DDR may post an enquiry to the parties concerning whether similar matters can be listed together or whether the matter needs to be listed for mediation. Two days before the callover the hearing is closed by the DDR and no further information can be posted. One day before the callover the Judge considers the documents received and will make orders concerning the listing and preparation of the matter for the Full Court hearing. The parties will be notified of the orders made via eCourtroom. If necessary, appropriate matters will be listed for a physical courtroom and removed from eCourtroom.

Access to eCourtroom is provided with two different levels. It is possible for any member of the public to link from the Federal Court website via the Electronic Services to eCourtroom. This will

[1223] As explained in Practice Note APP 1 the list of appellate sittings is called over before a Judge or a Registrar. At that time the parties must advise the Court about the nature of the matter, the essential issues and how they arise, as well as the nature of any cross appeal filed. Other issues to be considered at the call over include: whether there is an interlocutory application to be dealt with; whether in an appeal to be heard by a single judge, a party requires a judge to consider if it may be appropriate for the matter to be heard by a Full Court; whether the matter is ready for hearing; whether the contents of the appeal book has been settled/approved; whether an electronic appeal it to be considered; the estimated duration of the hearing; names of counsel briefed to appear and whether they have other matter listed in the same Full Courts; dates of proposed sittings when parties or their representatives are not available for hearing and the reasons for this; also any other details that may affect the listings such as whether the hearing needs to be expedited or whether the appeal raises a particularly important issue of law.

give access to the public transcript on eCourtroom. However, to participate it is necessary to register and access through the Commonwealth Courts Portal[1224] using a log on, as illustrated below:

Figure 1: **Public access to eCourtroom**

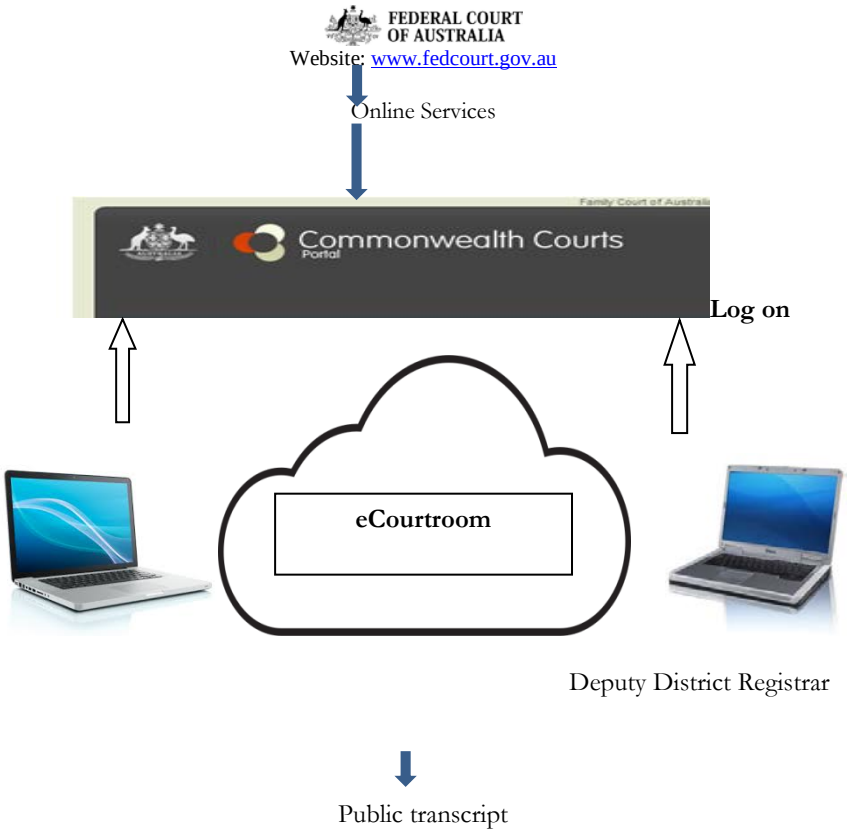


This diagram represents the limited access to online documents made available to non-parties to litigation. Access to eCourtroom is from the Federal Court website. The eCourtroom page provides a link to the public transcript without the necessity for logon. The search facility allows file searches using jurisdiction, file number and status (whether an active or inactive file). The parties' names and file numbers are listed. These details can be entered into the Federal Law Search facility on the main Federal Court webpage to provide further details about the cases.

[1224] Commonwealth Courts Portal website <https://www.comcourts.gov.au>.

[1225] A transcript facility on eCourtroom provides a record of all messes posted by the presiding Judicial Officer or Deputy District Registrar and the parties in any matter. This transcript is viewable by parties as well as the public. However, documents posted or filed can be viewed by the parties to the action only, the Judicial Officer, the Deputy District Registrar and other Court officers.

Figure 2: **Access to eCourtroom for parties**



This diagram represents the full online access provided to parties. It is necessary for the parties to register and then logon to enable them to participate in eCourtroom and lodge documents electronically.

In the following section I will examine five matters heard in eCourtroom in 2014 as case studies to assess the way such a virtual court operates from the information available to the public. The second analysis will be a detailed qualitative analysis of interviews, which presents data from the perspective of the Deputy District Registrars conducting the hearing.

5.4.2 Case studies of eCourtroom

The public transcript of five matters listed on eCourtroom in 2014 were selected for analysis, one from each category, as representative of the relevant categories of cases heard in the Federal Court and Federal Circuit Court of Australia. Three cases analysed were selected from the matters listed in 2014 in the Federal Court of Australia, one from each of the following categories: substituted service in bankruptcy; public examination of a company in liquidation; and a matter listed in the Appeals Callover list. Most, if not all matters listed in eCourtroom in the Federal Circuit Court are

bankruptcy matters, involving applications for substituted service. Two such matters were selected. The first was an application for substituted service of a creditor's petition where the application was successful and in contrast, in the second application, further evidence was required before the application was granted.

In addition to the qualitative analysis of the transcript a questionnaire was designed to analyse the experiences of legal staff of the Courts in their use of eCourtroom. In 2014 there were 24 matters listed in eCourtroom for the Federal Court of Australia, 11 listed in the New South Wales Registry and 13 listed in Victoria. Three matters were appeal actions, six Corporations actions and thirteen Bankruptcy actions. The number of listings and the time over which the matter is heard varies according to the complexity of the issues. The questionnaire was sent to the Registrars in the second half of 2014.

The following section contains the case studies from 2014 on substituted service in Bankruptcy matters, a public examination of a company in liquidation and an appeals matters to be listed in a Full Court sitting in 2014. They elucidate the advantages of virtual courts, such as eCourtroom in providing time and cost savings in that the matters are dealt with online and the parties do not have to appear in a physical courtroom. Access to the courts and security is facilitated by registration of the parties and online logon. The reference to personal information is limited. It has been anonymised for the purpose of the study. Despite the limited amount of personal information, the risk lies in the aggregation of data possible online. Information from the public transcript page of eCourtroom, together with personal data obtained from a Federal Court search, general searches on Google and OSNs, such a Facebook and Twitter, have the potential to lead to overexposure of personal data and invasions of privacy.

5.4.2.1 Case A – Federal Court: Bankruptcy – substituted service

This was an application for substituted service in Bankruptcy which was listed as an interlocutory hearing. The virtual courtroom was opened by the Registrar as follows:

> Dear Applicant,
>
> This is the eCourt hearing of an application for substituted service orders in respect of a creditors petition.

> It is proposed that the issues relevant to the making of these orders will be dealt with on-line through *eCourtroom* part of *eCourt* without the need to incur the costs of a court appearance. The *eCourtroom* hearing for this matter will open from today and will close when orders have been made.
>
> I now invite you to provide me with any further evidence and/or your submissions you wish me to consider in determining whether to make the orders you seek. Any documents sent to me via *eCourtroom* should be sent in Microsoft word .doc) or (.pdf) format.
>
> Would you also provide me with a draft of the orders you wish me to make in this matter. This document MUST be sent to me via *eCourtroom* in Microsoft WORD (.doc) format. Attached is a form of orders you may wish to consider in drafting your draft orders.
>
> I note the eCourt date for this application is [day/month] 2014. Please send me your draft orders by that date.
>
> Registrar

The Registrar has outlined the procedures to be followed and provided information to allow the applicant lawyer's to respond. The response was received on the same day.

> Dear Registrar
>
> Please find attached copy of draft orders sought by the applicant.
>
> With respect to any further evidence, we today filed a further affidavit of attempted service of Mr Y affirmed [day/month] 2014.
>
> The applicant does not intend do [sic] make any submissions, other than to say that XX Lawyers have acted for the respondent since [month] 2014 and appeared before Justice Y in the bankruptcy proceedings. Should it be deemed to be of any assistance to the court to make any formal submissions, we will do so forthwith. Kindly advise how you wish for us to proceed.
>
> Regards
>
> XX Lawyers

The following two responses on the following day clarified that no submissions would be required. Final orders were made four days after the eCourtroom had opened as follows:

> Dear ……

I refer to the affidavit filed in support of this application and advise that I am satisfied on the evidence to make the orders you seek.

Orders will be made in terms of the attached "Final" Orders. Please check them as there are some changes from your draft version. Unless otherwise advised the sealed orders will be sent to your office by post.

Please note that attendance at the Court Registry to amend the petition prior to sub service will be required.

eCourtroom is now closed. Further conduct of this matter will be dealt with in open Court.

Registrar

This matter was managed with the formality expected in a physical courtroom. The issues were resolved quickly, despite some changes to the orders, indicating time savings in comparison to a physical court hearing. Instructions to the applicant were clear in the written communication and, as the answers to question 3 indicate, there is a 'greater clarity in detailing' the matter. The efficiency, communication and procedural themes reflected in the Registrar's responses to question one in section 5.4.3.3 were demonstrated in this case study.

5.4.2.2 Case B – Federal Court: Corporations - examination

This matter was listed on a Thursday [month one, 2014] for public examination of a company in liquidation. It was not finalised for nearly six weeks. The issues were more complex. There were 12 postings in total. It was necessary to determine various dates for summonses to be issued and a return date set. The procedure for notification of examinees of the listed dates for the examinations in person was explained. The matter was opened in eCourtroom as follows:

I now convene this eCourtroom proceeding.

I have read the application for summonses for the production of documents and the affidavit in *support. Subject to the matters raised below, I am willing to issue summonses to the proposed* examinees, [names of examinees listed].

1. The definition of "books and records" in the Schedule to the summonses for Mr and Mrs X and Ms Y are extremely wide. In my experience, this can encourage delays in the process, particularly where the suggestion is that electronic archives must be searched. The applicant may wish to consider whether

he really seeks every scrap of paper at this stage, or whether it might be possible to narrow the scope of the definition.

2. It is not apparent what requests have been put to the various examinees for production of the documents. It is always preferable to pursue documents through ordinary written requests first, rather than court process…
3. …
4. With regard to the personal information sought, once again, the width of the definition of all books and records relating to the examinees personal financial circumstances may throw up more documents than the liquidator really requires. For example, would the Income Tax Returns be sufficient, rather than all the books and records that may be have been created in the process of preparing those returns? Would a statement of financial affairs providing details in relation to the listed matters be more effective than boxes of documents and CDs of emails and texts? Please advise whether the applicant is prepared to limit the scope of the documents sought in each of the summonses to avoid possible delay while the examinees undertake time consuming searches?

…

Please advise of the applicant's response to the above matters by return posting.

Registrar

The applicant's lawyers responded six days later explaining the reason for the delay and replying to the Registrar's queries.

Dear Registrar ….

I apologise for not responding to the Registrar earlier. I was having some technical issues accessing eCourtroom.

With respect to point 1, the definition of "Books and Records" was taken from the Corporations Act and was included in our public examination Summonses as standard practise on the advice of another Registrar in another public examination matter.

If the Registrar thinks in this instance, that definition is too broad, I will seek instructions to remove it or narrowing the scope of the definition.

With respect to point 2, there has not been any formal request for these documents.

…

With respect to point 4, if the Registrar deems this too wide, I will seek instructions to amend it.

…

Kind regards

ZZ Lawyers

In the posting two days later the Registrar stated that 'without some compelling urgency, I would not approve the issue of summonses for production where no written requests have been made beforehand'. The applicant's lawyers were advised that they should seek instructions concerning whether a narrower range of documents would be sufficient or whether 'all possible documents, notes, electronic documents, notes, scraps of paper etc' were sought. The applicant was informed that some of the requests were 'partly a fishing expedition' and the Registrar commented, '[l]iquidators are entitled to a certain amount of fishing in public examination' asking the applicant's lawyers to seek instructions about whether it would be necessary to 'go back 3 years to determine whether there is a pattern of like dealings between the relevant individuals and entities … '

A week later the applicant's lawyers replied to the Registrar that he was writing to the examinees concerning their documents, attaching copies of previous correspondence and sought advice as to whether 'a more formal request for the exact documents sought' in their draft summonses would be required. There was a delay of about four weeks before the Registrar responded to provide information about the draft summonses. The delay was attributed to either personal error or 'some technical glitch'. A further seven exchanges over a week followed detailing the dates for production of documents and various listings, including closing the eCourtroom.

This matter required more postings than A or C. There was an indication that there were technical difficulties by both the Registrar and the applicant's representative. There was also some indication that the formality of the proceedings was challenged by the response to the Registrar's comments on the definition of 'books and records'. The more complex procedure reflected the Registrars' responses to question 3 in section 5.4.3.3 where there was some indication that a normal court hearing may be better for such matters and that a virtual court may not be the best medium.

5.4.2.3 Case C – Federal Court: Appeals – eCourtroom Callover

The matter concerned the listing of an appeal matter for one of the Full Court and Appellate sitting periods in 2014. The courtroom was opened by a legal officer of the Federal Court on behalf of the Registrar as follows:

Dear practitioners

This is the callover for the Full Court and Appellate sittings for the period [days; month] 2014.

> It is proposed that issues relevant to listing this matter for hearing during the Full Court and Appellate sittings will be dealt with on-line through *eCourtroom* without the need to incur the cost of a court appearance. All information posted on *eCourtroom* is available for public transcript.
>
> The *eCourtroom* Callover of this matter will be open from today and will close on [day, month] 2014.
>
> If not already done a Status Report for Full Courts and Appellate Matters should be sent **as soon as possible.**
>
> Parties are also invited to advise the Callover Judge (XX CJ) of any further matter regarding the listing of this matter in the above sittings period (*other than what has been set out in your Status Report*) or provide proposed consent orders in relation to the future conduct and/or listing of this matter for hearing. Communications of this nature must be received via *eCourtroom* by the above date.
>
> Orders for the future listing and preparation of this matter for hearing will be notified to you on or shortly after [day;month] 2014.
>
> Registrar

The second posting requested the practitioners to upload their status report. This was complied with by the appellant's lawyers on the following day.

This matter indicated that the procedure in eCourtroom works well in matters that involve uncomplicated procedural issues. In this instance the purpose for the hearing was to determine if the parties were ready to proceed to a full court hearing in the next available sitting period. There was a request for a status report from the parties. Once there was compliance the orders for the listing were made. The hearing was determined quickly without any necessity for the parties to attend a physical court hearing. It can be contrasted with B in which there were alleged technical difficulties and complexities relating to the requests for the production of documents. The Registrars' responses to the questionnaire in section 5.4.3.3 support the conclusion that eCourtroom is best suited to uncontested applications and procedural issues.

5.4.2.4 Case D – Federal Circuit Court of Australia – application for substituted service

In 2014 the public transcript of eCourtroom indicated that there were 629 matters heard in the Federal Circuit Court of Australia. These were almost all applications for substituted service in bankruptcy matters. The following cases provide an indication of the process in action.

a) This case concerned an application for substituted service of a creditor's petition. It was selected randomly from the 2014 matters. The eCourtroom was opened as follows:

> Thursday […] 2014
>
> I now convene this eCourtroom hearing.
>
> I have reviewed the application for substituted service of Creditor's Petition No [WWXY] and the affidavit in support. I am generally satisfied that the method of substituted service sought in relation to the email address abcd@gmail.com and the mobile telephone number [……..], and provided for in the attached draft order will, in all reasonable probability, be effective in bringing knowledge of a valid creditor's petition to the attention of the respondent debtor, [XX]. In light of this, it is unnecessary to also post documents to [ABD Street …]. Accordingly, I am prepared to make orders in the form of the attached draft order.
>
> I note there is an error in the title of the Interim Application filed by the Applicant. In my view, that has no material effect on the application. Nevertheless, I have provided for an order correcting it in the attached draft order.
>
> Please indicate by posting a response whether you have any objections to any matters specified in the draft order, and if no, on what basis.
>
> In the ordinary course, sealed orders would be posted to you. Please indicate in your response whether you would prefer to pick the sealed orders up from the Registry.
>
> Registry

There was a response from the applicant on the following day indicating that they had no objections and they would collect the sealed orders from Registry. On Monday the Registrar indicated that the orders were ready for collection and that there was a minor amendment to the order. The eCourtroom proceeding was closed having been finalised within four business days.

b) Not all applications were successful at first. Some applications required further evidence such as the following:

> I now convene the eCourtroom for the application filed on XX August 2014 seeking an order for substituted service of a bankruptcy notice.
>
> Before orders for substituted service will be made, the Court must be satisfied of the following:
>
> 1) That abnormal difficulties exist in serving the bankruptcy notice in a manner prescribed by sub-regulation 16.01(1) of the Regulations; and

2) There is a reasonable probability that the debtor will be informed of the bankruptcy notice as a result of the form of service proposed.
There is no sworn evidence from the process server about his attempts to serve the debtor or of conversations he had with any persons. The only evidence is hearsay.

The email received from the process server makes reference to a conversation with the security guard at the XXX address. The security guard advised that a "Mr ABC" is on their list for that address. But there is no evidence to support that is one and the same Mr ABC named in the bankruptcy notice. Further evidence is therefore required to support this application. I will adjourn the application until [XX date] at 3 pm (eCourtroom) to allow the applicant time to file further evidence.

Registrar XY

The matter was relisted at a later date and the application dismissed approximately 15 months later. There were no further public transcripts available on the Commonwealth Courts Portal and no indication if the application was finally dismissed for lack of evidence. The public transcript of other eCourtroom matters indicates quite a rigorous questioning of the applicant's lawyers for evidence in support of their application for substituted service. The comments and questions by the Registrar requestion details about the nexus between the address and the debtor such as land title searches and inquiries of other authorities; details about the mobile number and work role of the debtor. After further affidavit evidence was filed responding to the Registrar's inquiries the application for substituted service was granted when the Registrar stated '[o]n the totality of the material in support, I am now satisfied that personal service of the creditor's petition is impractical … '.

These matters for substituted service in the Federal Circuit Court were managed in a similar manner to Case A in the Federal Court and managed with the formality of a physical courtroom, although the Registrars' responses indicated there had been some informality in replies in the early days of eCourtroom use. Access to the courtroom was efficient and savings in time and cost provided by parties participating from their desks rather than in a physical courtroom. A few technical issues emerged as indicated in the response to Case B in section 5.4.2.2. Communication was clear and recorded for the benefit of parties and the public. It is possible to conclude that access to justice, particularly for procedural matters such as applications for substituted service in Bankruptcy was enhanced by the use of eCourtroom.

The following section will present an analysis of interviews conducted with Deputy District Registrars of the Federal Court and Federal Circuit Court conducted in November and December 2014. The aim of the research was to provide a more complete assessment of the use of eCourtroom, particularly from the perspective of the users and to develop an understanding, together with the results of the case studies, about whether this process provided enhanced access to the courts as well as protecting the security and privacy of personal information.

5.4.3 Qualitative content analysis: eCourtroom interviews

5.4.3.1 Methodology

The use of qualitative content analysis was chosen to assess the Registrars' responses to a questionnaire and to present a more complete analysis of virtual courts together with the case studies. Qualitative content analysis is a form of analysis used to focus on 'the characteristics of language as communication with attention to the content or contextual meaning of the text' to provide a more comprehensive understanding of the phenomenon studied.[1226] It has been defined as 'a research method for the subjective interpretation of the content of text data through the systematic classification process of coding and identifying themes or patterns.'[1227] While numerous approaches to qualitative content analysis have been described they all require a similar analytical process.[1228] A conventional content analysis was chosen to analyse information about the experience of Registrars using electronic litigation.

Hsieh and Shannon refer to 'seven classic steps' in content analysis when describing the three approaches to qualitative content analysis,[1229] in comparison with the five step process in framework analysis. I have also used five main steps in this analysis: the first, the formulation of the questions; the second, the sample selection; third, the coding; the fourth, the analysis of the data using the codes and criteria; and finally an assessment of the validity and reliability of the process.

[1226] Hsiu-Gang Hsieh and Sarah E Shannon, 'Three Approaches to Qualitative Content Analysis' (2005) 19 *Qualitative Health Research* 1277-1288, 1278.

[1227] Ibid.

[1228] Ibid, 1279-1286. In this article, Hsieh and Shannon refer to 'conventional content analysis' (where the codes are derived from the data), 'directed content analysis' (where the codes are derived from theory) and 'summative content analysis' (where the codes are derived from the interest of researches or from a review of the literature). The methods also differ in where the studies start and the timing of defining codes or keywords. A more prescriptive method of qualitative content analysis, Framework analysis, was developed by the Social and Community Planning Research Institute, London, by Jane Ritchie and Liz Spencer in 1994. It was developed specifically for applied policy research and is primarily used in health care. This method uses five steps for process analysis and aims to generate recommendations or outcomes within a limited period of time on given policy issues: See Aashish Srivastava and S Bruce Thomson, 'Framework Analysis: A Qualitative Methodology for Applied Policy Research' (2009) 4 *Journal of Administration & Governance* 72-79.

[1229] Hsieh and Shannon, above n 1226, 1285-1286.

The first step: the formulation of the questions was undertaken with a consideration of my research topic and research main question – the extent to which Web 2.0 applications should be used to enhance access to justice. A detailed list of the questions and analysis follows. They are directed to eliciting responses from the Registrars about their experience using the virtual court, related issues such as protection of personal data and the use could be extended. The second step: the sample selection, was dictated more by the limited number of Registrars using eCourtroom and the possibility that all Registrars would complete the questionnaire.

The third and fourth steps, the coding and analysis were the most challenging and time-consuming steps in the process, however, these steps were applied to provide a systematic analysis of the responses. Manifest coding was applied which focusses on whether a word or theme is present or not. It does not take the connotations of the words or phrases into account.[1230] I read and familiarised myself with all 21 responses from the Registrars to 'pull out emerging themes' which become codes.[1231] The responses were organised into responses for each question to facilitate a focus on each theme and category identified. To assist in the detailed analysis, descriptive phrases and words, such as 'save costs', 'easy to use' and 'text focussed' were isolated from the responses to each question.[1232] Six categories were identified from these phrases: these were; 'procedure', 'communication', 'efficiency', 'technology', 'administration of justice' and 'privacy'.[1233] These categories demonstrated some duplication of ideas. Additional categories, such as 'representation' and 'practitioners' were identified initially but were discarded due to overlap in concepts and the decision to focus on six main themes.

Because such data has been found to be 'invariably unstructured and unwieldy' this methodology was used to 'provide some coherence and structure … while retaining a hold of the original accounts and observations from which it is derived'.[1234] Berg and Lune have argued that content analysis can be effective in qualitative analysis by providing 'a passport to listening to the words of the text, and understanding better the perspective(s) of the producer of these words'.[1235]

[1230] W Lawrence Neuman, *Social Research Methods: Qualitative and Quantitative Approaches* (Allyn & Bacon, 2000, 4th ed) 295.
[1231] Webley, above n 244.
[1232] See Appendix C.
[1233] See Appendix C.
[1234] Jane Ritchie and Liz Spencer, 'Qualitative Data Analysis for Applied Policy Research' in A Michael Huberman, Matthew B Miles (eds) *The Qualitative Researcher's Companion* (Sage Publications, 2002) 309.
[1235] Bruce L Berg and Howard Lune, 'An Introduction to Content Analysis' Chapter 11 in *Qualitative Research Methods for the Social Science,* (Peachpit Press, 8th ed, 2011), 238, 240.

Where large numbers are involved, computer analysis can be of great assistance in coding,[1236] however, in this analysis, the small number of Registrars that use eCourtroom made the use of computer analysis unnecessary. It was possible to present a detailed qualitative analysis and interpretation of the data obtained using manual methods.

The fifth step, the validity and reliability of the methodology was addressed within the suggested framework for achieving quality in qualitative research in mind. Tracy has identified eight 'big-tent' criteria: a worthy topic; right rigor; sincerity; credibility; resonance; significant contribution; ethics and; meaningful coherence.[1237] In analysing the eight criteria, Walby and Luscombe considered that there was some crossover in them as they are not totally distinct, however, the primary goal must be to 'be open and honest about the strengths and limits of research'.[1238] Golafshani has discussed the use of reliability and validity in qualitative research and the application of triangulation.[1239] He considered that using multiple methods 'will lead to more valid, reliable and diverse construction of realities'. Johnson and Onwuegbuzie were also supportive of mixed methods research providing pluralism and frequently superior research by providing complementary strengths.[1240] It is for these reasons that multiple methods were adopted for the analysis of eCourtroom, case studies and a questionnaire to supplement the theoretical analysis and provide triangulation and validity to the research findings.

5.4.3.2 The questionnaire

Ethics approval was sought from the Faculty of Arts Human Research Ethics Committee, Macquarie University. This was granted on 28 July 2014 (see Appendix A). The questionnaire consisting of five questions were sent to all District and Deputy District Registrars[1241] of the Federal Court and Registrars of the Federal Circuit Court ('the Registrars')[1242] by email on 17 November 2014, together with a consent form (to be signed and returned) and a dissertation abstract to explain

[1236] Computer assisted qualitative data analysis software (CAQDAS) refers to a wide range of analysis software which supports a variety of analytic styles in qualitative work <http://atlasti.com>.
[1237] Sarah J Tracy, 'Qualitative Quality: Eight "Big-Tent" Criteria for Excellent Qualitative Research' (2010) 16 *Qualitative Inquiry* 837-851, 839.
[1238] Kevin Walby and Alex Luscombe, 'Criteria for quality in qualitative research and use of freedom of information requests in the social sciences' (2016) 1 *Qualitative Research* 1-17, 6-11.
[1239] Nahid Golafshani, 'Understanding Reliability and Validity in Qualitative Research' (2003) 8 *The Qualitative Report* 597-607.
[1240] R Burke Johnson and Anthony J Onwuegbuzie, 'Mixed Methods Research: A Research Paradigm Whose Time Has Come' (2004) 33(7) *Educational Researcher* 14-26.
[1241] The Deputy District Registrars of the Federal Court are also appointed as Registrars of the Federal Circuit Court. The Deputy District Registrars based in Sydney are also Deputy District Registrars of the A.C.T. Twenty seven Registrars were identified as having the capacity to use eCourtroom. The Registrars are not evenly distributed throughout Australia. There are seven in NSW and Victoria, four in Queensland and Western Australia, two in South Australia and one in Tasmania.
[1242] The Deputy District Registrars and Registrars will be collectively referred to as the Registrars.

the reasons for the questionnaire. All the Registrars were asked to respond to the same questions to enable a comparison to be made and more generalised results obtained. The Registrars were able to respond however they chose to without the restriction of selecting a fixed range of responses. The questions were designed to encourage open-ended responses.

The goals of the research were explained to each Registrar and the confidentiality regime adopted for the responses. Two Registrars chose to respond by phone. The majority responded by email within one month. A few Registrars indicated that they had nothing to contribute because they had not been using eCourtroom. The responses were collated by mid-December 2014.

The overall response rate was very high at 81%.[1243] The response rate from the larger registries (NSW and Victoria) was 92.8% and lower from smaller registries such as Queensland and Western Australia (50%) however there was a very high response rate from South Australia (100%) where there were 2 Registrars. Some of the results reflected the degree of use of eCourtrrom in different registries. The eCourtroom information available on the Commonwealth Court Portal indicates that the majority of matters were filed in the Federal Circuit Court of Australia and in the Sydney Registry, although there was substantial use in the Victorian Registry.

The questionnaire consisted of the following questions:

1. *Can you tell me generally about your experience hearing matters for either the Federal Court or the Federal Circuit Court of Australia in eCourtroom?*

2. *What have you found to be the advantages of dealing with applications for substituted service by electronic litigation rather than in a physical courtroom?*

3. *Have you found any disadvantages or issues in using eCourtroom for such applications? When do you consider it would not be appropriate?*

4. *A live public transcript of proceedings is available online. What other access do you consider third parties should have to documents relating to eCourtroom matters? Is there anything peculiar to substituted service that requires privacy or confidentiality?*

[1243] The response rate from the Registrars was possibly high due as I had worked as a Registrar in the New South Wales Registry and knew them all personally. Two of the Registrars responded by phone rather than by email. Three stated that they did not use eCourtroom and one stated that the use was limited. Three Registrars stated that they didn't use eCourtroom. There was no response from five of the 21 Registrars contacted.

5. *Do you consider eCourtroom to be useful for any other matters? Would your opinion change if you could use skype-like facilities to communicate with the parties?*

The questions chosen were designed to cover issues relevant to the research question and were designed to explore the general nature of the use of a Web 2.0 application in Australian courts, particularly any advantages or disadvantages perceived by the Registrars as users of the system. Question 4 was directed more specifically at the issue of privacy and the extent to which personal data is made available to the public online. The final question was directed to the future use of eCourtroom and what difference the use of skype-like facilities might make in extending the use to other than procedural hearings. Additional questions could have been directed the issue of data retention and reduction, including the responsibilities of the courts and parties for the protection of personal information due to the permanence of digital records. However, I considered that a short questionnaire would elict more immediate responses from busy participants such as Registrars and give some indication of the feedback and possibilities of research in the future.

5.4.3.3 – Responses: qualitative content analysis

Passages of responses were examined to identify any themes that may have emerged. Responses to each question were extracted from each Registrar's comments and examined together, so that all responses to question one were examined, followed by responses to question two – five. The data was coded [Appendix C] to identify the most important themes and this was related to the main issues being examined by the research question – access to justice, privacy and technology. The main categories emerged from the initial coding of responses. These were efficiency, procedure, communication, privacy, technology and access to justice.

1. *Can you tell me generally about your experience hearing matters for either the Federal Court or the Federal Circuit Court of Australia in eCourtroom?*

This was a general open-ended question to elicit an overview of the impression the use of eCourtroom had made on the Registrars as users of this virtual court. The main category identified in analysis of the responses to this question related to efficiency and procedure. The most common use of the courtroom was for ex parte applications for substituted service applications in bankruptcy, examinations in bankruptcy and insolvency in corporations law, particularly in the Federal Circuit Court of Australia rather than the Federal Court.

Comments referred to the procedure as 'an efficient way of dealing with substituted service applications', as 'a very useful tool' and one that 'is working very well with the standard being quite high'. One Registrar commented that 'occasionally … communications from practitioners to registrars were overly informal or personal', however this was largely rectified by reminding practitioners in the introduction to eCourtroom that the process is a court hearing and communication should remain the same as in a physical courtroom: this was a reference to the eCourtroom Protocol which is available on the Federal Court website.[1244]

A number of Registrars commented on the savings in costs as well as the 'greater flexibility in time'. One Registrar explained that that eCourtroom enabled the parties to save costs, provided them with greater flexibility in time and avoided the necessity of a face to face hearing. The advantages of written communication and eCourtroom as a 'text focused' were referred to in response to the first question. These issues were dealt with in more detail in the responses to question 2 (see below).

One Registrar referred to having a 'very sceptical' attitude when eCourtroom was first introduced but subsequently, particularly following improvements in the technology, found it worked well. There were a few Registrars who had limited experience with eCourtroom, so were unable to contribute much to the questions. Only one considered that eCourtroom was not necessarily the best medium for hearing applications when they could be 'dealt with more efficiently in the normal court room', and made the following comments: The eCourtroom hearing was found to take longer 'to convert one's thoughts into the written form than to express those thoughts orally'; also the applicants were 'naturally prone to analysing what is written in more depth before responding'. It was also considered that there seemed to be no need for the party to respond immediately which caused delay. This problem is highlighted above, in Case B above which was not finalised for nearly six weeks.

The main themes identified in response to this question were the efficiency, the nature of the procedure and the difference communication path provided by the virtual court. The savings in costs and time were found to contribute to the efficiency of the process.

[1244] The language and modes of address used on the eCourtroom must be the same as that used if the matter were being dealt with in an ordinary courtroom: <http://www.fedcourt.gov.au/online-servcies/ecourtroom/protocol>

2. *What have you found to be the advantages of dealing with applications for substituted service by electronic litigation rather than in a physical courtroom?*

In referring to the advantages of using the virtual courtroom the most common categories identified were efficiency and communication, with some repetition of the issues discussed in the responses to question 1 with comments such as 'greater flexibility', 'not time sensitive', 'there is a detailed written record of the proceeding' and 'not bound to a specific date and time'. The issues of cost efficiencies were mentioned in terms such as: 'save costs to parties in avoiding face to face attendance at Court', 'some costs savings to the Court in the reduction of use of court facilities and the need for attendance of court officers' and 'not a burden on firms and they can pass savings on to clients, charge relatively low rates'. One Registrar considered that the eCourtroom process was 'important for a national court' because participation can be 'from anywhere'. Another referred to efficiencies in listing because 'we can list them much sooner than in a physical court room', 'hold a 'list' once a week' rather than have a time delay of a week from the date of filing to listing date. Flexibility in listing allows Registrars to list urgent matters quickly and the hearing time for each matter was more flexible. Time savings in 'not needing to open a physical court for the hearings' was also mentioned. There was also mention of the flexibility for the parties and Registrar in not being 'bound to a specific date and time for dealing with the proceeding'. The eCourtroom process was seen as a 'better use of everyone's time', particularly as 'sub service orders are quite long and can be complex'. Time and cost savings were addressed in mention of the savings to parties and practitioners in not having to appear in a physical courtroom.

The advantage of having a 'detailed written record', not usually be taken for such proceedings and the 'greater clarity in detailing the matters' in written communication was also seen to provide 'greater consistency when stating my view of how the law is to be applied in the particular case'.

The use of technology was seen as an advantage in that eCourtroom '[e]mbraces use of technology in a court environment'. This was particularly useful '[o]nce you get familiar with the software' then the process is quicker and can be 'done at my convenience when I have some free time'.

3. *Have you found any disadvantages or issues in using eCourtroom for such applications? When do you consider it would not be appropriate?*

The categories of procedure and efficiency were the focus of the responses to this question. Some of the disadvantages related to the process and the difficulties some Registrars faced in explaining that eCourtroom was 'not just an email chat room' but a formal court process. When the legal representatives were inexperienced with a substituted service order they required a 'lot of 'hand-holding' through the process which led to inefficiencies. The comment was also made that in the field of insolvency 'the majority of matters are dealt with by small firms, less experienced practitioners' and some firms even use 'clerks and trainee lawyers'. It was considered that self-represented parties, unfamiliar with court procedures, 'may not be willing to have their matters dealt with this way'.

A few technological disadvantages were discussed such as, [t]he need to 'be IT savvy and have good keyboard skills' and the problems that arise when 'parties/practitioners may not have the IT capability to support eCourtroom forum'. Another technical disadvantage mentioned was one relating to 'the computer program which does not … allow for a second response and requires a separate word document to be open and pasted in to the conversation'. The Registrar mentioned that 'this may be as a result of my limited computer skills'.

It was considered that 'eCourtroom not appropriate for dealing with complex matters that may require consideration of complicated orders'. One Registrar commented that it was preferable for the applicant's lawyer to physically appear in court to enable immediate responses 'where there are issues regarding the sufficiency of the evidence'. Another referring to the problem of answers that are 'too cumbersome to communicate by email'. This required a relisting of the matter in a physical courtroom on a future date, however this was considered a 'rare' occurrence. As well when complex submissions were required, eCourtroom was sometimes not appropriate. This was also expressed by another Registrar as appropriate where 'there are factual disputes or cases where the court would benefit from oral submissions to parties'.

4. *A live public transcript of proceedings is available online. What other access do you consider third parties should have to documents relating to eCourtroom matters? Is there anything peculiar to substituted service that requires privacy or confidentiality?*

The categories most prominent in the analysis of the responses to question four were privacy and access to justice. Particular responses identified access to the transcript by third parties and issues of confidentiality or privacy that may be peculiar to substituted service.

Most Registrars considered that access to documents for third parties should be the same in eCourtroom as the physical courtroom, so that 'eCourtroom mirrored what happened in open court'. Another commented that they were 'content with the existing arrangements under r 2.32 for access to documents'.[1245] Also the comment was made that it was important for 'third parties to have the same level of access to documents as they would have in a proceeding conducted in the physical court room'.

There was some consideration of the limitations that may be required in substituted service applications, particularly 'as a respondent may make himself/herself unavailable' when it is known how the service was to be effected. Other comments included that the fact that if the respondent was aware of the substituted service, then the person may 'go to ground', with examinations in bankruptcy and corporations matters, particularly if there is fraud 'money would be moved out of the company' and the 'respondent may get rid of evidence' if they know about the proceedings. In this case it was thought that it would be better if the respondent was not aware of the public transcript. Another Registrar considered that despite the difficulties of the respondent possibly avoiding service, 'this is balanced by the fact that communication to the respondent may put them on notice that service may be effected whether they make themselves available or not'.

A few of the Registrars mentioned that some of the personal details, such as, 'the whereabouts, living arrangements or personal circumstances of a respondent may not be suitable for publication'. Also information about mobile phone numbers, home or work addresses and email addresses, while 'potentially private', it was considered that these details are available in open court and 'in open court these details are in the public domain'. The comment was made that:

[1245] This refers to rule 2.32 of the *Federal Court Rule 2011* (Cth) relating to the inspection of documents. It provides: '(1) a party may inspect any document in the proceeding except: (a) a document for which a claim of privilege hs been made: (i) but not decided by the Court; or (ii) that the Court has decided is privileged; or (b) a document that the Court has ordered be confidential. (2) A person who is not a party may inspect the following documents in a proceeding in the proper Registry: (a) an originating application or cross-claim; (b) a notice of address for service; (c) a pleading or particulars of a pleading or similar document (d) a statement of agreed facts or an agreed statement of facts; (e) an interlocutory application (f) a judgment or an order of the Court; (g) a notice of appeal or cross-appeal; (h) a notice of discontinuance; (i) a notice of change of lawyer; (j) a notice of ceasing to act; (k) in a proceeding to which Division 34.7 applies: (i) an affidavit accompanying an application, or an amended application, under section 61 of the *Native Title Act 1993*; or (ii) an extract from the Register of Native Title Claims received by the Court from the Native Title Registrar; (l) reasons for judgment … (3) However, a person who is not a party is not entitled to inspect a document that the Court has ordered: (a) be confidential; or (b) is forbidden from, or restricted from publication to, the person or a class of persons of which the person is a member … (4) A person may apply to the Court for leave to inspect a document that the person is not otherwise entitled to inspect. (5) A person may be given a copy of a document, except a copy of the transcript in the proceeding, if the person: (a) is entitled to inspect the document; and (b) has paid the prescribed fee … '

> applications for substituted service (or more correctly the evidence in support), however, are more **likely to contain personal and sensitive information about individuals** … than contained in other filed documents which could inappropriately be used for 'identity theft' or other possible infringements of individual privacy.
> (emphasis added)

The availability of the written transcript on the Federal Court intranet raised a few issues. It was felt that 'care must be taken to ensure that certain personal information of a party is not reproduced therein, in the same way that care might be taken in the physical court room to ensure that certain personal details do not end up on the public transcript'. It was considered that 'the public transcript gives these matters a very much wider exposure than they would otherwise have had if dealt with in chambers'. It was thought that there could be extreme cases where 'somebody has escaped (for example a violent domestic situation and for that reason does not want his/her current whereabouts to be known to the ex-partner'.

Comments regarding the solution to privacy issues included, 'third party access to final orders should be restricted'; 'it would be appropriate to redact the evidence before allowing any third party access'. Although a party, attempting to avoid service could access eCourtroom to check if any orders had been made, it was thought that, '[h]ving regard to the fact that service is usually deemed to occur on the happening of certain events the knowledge of the party attempting to avoid the service is not relevant'.

There was some indication from the responses that a further exploration of the protection of personal data, particularly post-litigation was needed. The issues that arose in *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (Case C-1131/12)[1246] (*Google Spain*) were related to personal debt recovery proceedings which had been reported in a newspaper and found to be available through a Google search a considerable time after the event. The possibility of personal financial details required for online court hearings being misused in the future would be an issue for further research. This study could include the possible protection that could be provided by a right to be forgotten or procedure that could provide a similar measure of protection as that found by the practical obscurity of past hard copy records.

5. *Do you consider eCourtroom to be useful for any other matters? Would your opinion change if you could use skype-like facilities to communicate with the parties?*

[1246] *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (Case C-1131/12) *(Google Spain)* below n 1450. For a more detailed discussion of *Google Spain*, see Chapter Six of this thesis.

The categories of procedure and access to justice were the main themes addressed in response to question 5. The other uses for eCourtroom discussed by the Registrars included: some directions hearings where there were minor issues that needed clarification and amendments; 'for mediations instead of phone appearance'; appeal index conferences; consent adjournment applications, setting down mediations; or 'for any application of a procedural nature that may require a judge or registrar to receive draft forms of orders'; '[m]atters being decided on submissions where there is no contested evidence'; and applications for extension of time.

While it was considered very useful in its current application '[i]t is not designed for contested applications as there is no facility for a three-way link'. Most Registrars expressed some interest in the extension of the eCourtroom technology to include skype-like facilities, considering the addition of such facilities as 'likely to assist in allowing the usual dynamics of human communication to become a greater part of the process'; to allow the extension to 'inter partes matters or matters where oral submissions are necessary as then it will not really differ from the video conferencing facilities that the court already uses'; possibly be a cost saving instead of using video links, and it could be used instead of telephone links. Although, it was considered 'unrealistic to have that expectation' because skype-like facilities would require all practitioners to have the same technology.

Other Registrars felt that it would be 'difficult to see eCourtroom having an application beyond ex parte applications' and that 'once you are using skype you might as well require parties to attend in person or by phone, which we currently allow'. In addition, it was considered that skype-like facilities are 'not yet sufficiently reliable not does every Court have the software available'. The comment was made that 'a controlled Court room environment' was often necessary 'to ensure the witness is not being prompted off camera'. This was a concern in *Rezaeipoor v Arabhalvai*[1247] where the decision by the Master to allow the use of Skype for the cross-examination of a crucial witness. The counsel for the claimant did not object to the use of Skype in principle, however, his concern was that adequate controls were not in place. The Master having allowed the decision to use this technology was careful to ensure that the witness was not given pieces of paper or interfered with when she gave her evidence. He found the Skype transmission very successful.

[1247] *Rezaeipoor v Arabhalvai* [2012] EWHC 146, is discussed in more detail in section 5.3.

5.5 The use of eCourtroom: analysis

In the analysis of the use of eCourtroom two methods were used, case studies and a questionnaire. The responses to the questionnaire by the Registrars, particularly where cost and time savings were discussed, generally support a conclusion that access to the courts is enhanced by using eCourtroom. It is also evident from the analysis of the public transcript that matters chosen for listing in eCourtroom were generally dealt with quickly and without the necessity of physical attendance in court. The flexibility in listing times added to the efficiency of the procedures.

As a means of communication with the courts, eCourtroom was found to be suited to the matters listed and it provided detailed written records, as seen in the public transcript available online. Some issues arose relating to the informality and discursive nature of responses from practitioners which appear to have been solved by reminders about the eCourtroom Protocol. The limitations of communication concerned some absence of the usual dynamics of human communication through visual and physical responses. It appeared that the written communication of eCourtroom was suited to the administrative procedures of applications for substituted service. More complex matters that required an assessment of the witness testimony were listed in the traditional courtroom. The application of eCourtroom to substituted service applications and administrative procedures has proven successful, particularly in the Registries dealing with larger numbers of applications and in the Federal Circuit Court of Australia. In its present form without the use of VoIP it did not appear to be as useful for more complex procedures and contested applications. However, it appears that there would be the potential for more extended use of a virtual court in the future as technologies and security measures are addressed.

The references to technical problems encountered by the Registrar and practitioner led to delays, although the delay may well have been caused by personal error rather than 'some technical glitch' which is an issue referred to in the Registrar's responses earlier. Some negative comments concerned the computer skills, particularly of some practitioners and paralegals and the limits of the computer programs. There was some support for extending the interactive technology to include VoIP or skype-like technology which may overcome the difficulties when face-to-face procedures were not possible. The question of whether Australian Courts should give more witnesses the right to Skype was considered recently by Krawitz and Howard.[1248] It was suggested that this proposal should be considered when video conferencing is not available, if factors such as increased security

[1248] Krawitz and Howard, above n 1207.

problems and opportunities for judicial officers to assess the credibility of the witnesses are considered, or as the UK judge found in *Rezaeipoor v Arabhalvai.*[1249]

There was an awareness of the sensitivity of some of the personal data, such as mobile phone numbers or email addresses and the problems that could be caused by general disclosure, although the need to provide open justice. The dilemma faced was, that while care had to be taken with personal information, it would be available in a physical courtroom. However the nature of the availability has changed due to the permanency of the internet's infinite memory. The availability of the public transcript indicated the Courts' support for open justice. In most cases in the Federal Courts a written transcript of the proceedings is available for purchase by the parties. Third party access to the transcript is set out in a Non-party Access to Transcript Protocol which provides that access will be granted where no order of the Court has restricted this access and a formal request on the approved form with payment of the relevant fee has been made to Auscript[1250]. Provision under a protocol is also made for the issue of a transcript to impecunious litigants when necessary for the administration of justice, determined by the Court.

A review of matters listed in eCourtroom in 2015 and in 2016 indicated there has been limited change in the use of eCourtroom since 2014. This virtual court is being used mainly for applications for substituted service in bankruptcy matters and for Full Court callovers to save the cost of a court appearance in uncomplicated matters. The number of listings in the Federal Court and Federal Circuit Court remains comparable to those listed in 2014.[1251]

What this research did not examine was the inadvertent disclosure of personal data or that produced by aggregation from combined searches on court websites, Google and OSNs, nor the issues that arose in *Google Spain.*[1252] The subsequent use and dissemination of information was discussed by Conley et al, particularly the use data aggregation services could make of information acquired from court records.[1253] This research was beyond the scope of the current investigation, however, it would have considerable significance for future research on the impact of online disclosure of personal data and privacy.

[1249] *Rezaeipoor v Arabhalvai* [2012] EWHC 146 (Ch).
[1250] Auscript Australasia Pty Ltd (Auscript), under contract, provides the transcript of most Federal Court and Federal Circuit Court proceedings, although the transcript remains with the property of the Commonwealth of Australia <http://www.auscript.com>.
[1251] The public transcript page indicated that there were 45 matters listed in 2015 and 43 (2 December 2016). Similar numbers of matters were heard in eCourtroom in the Federal Circuit Court in 2014 (687), in 2015 (625), however, in 2016 there were fewer matters listed (436) to 2 December 2016.
[1252] *Google Spain* below n 1449.
[1253] Conley et al, above n 292, 812-813.

Further research on the application of eCourtroom could include use of interactive, audio-visual technologies such as VoIP in more complex matters. A more comprehensive analysis could also include responses by practitioners similar to the questionnaire sent to the Registrars. There is considerable scope for future research, particularly as the applications of interactive technologies such as eCourtroom are developed in the future.

5.6 Conclusion: Virtual courts providing access and privacy

The expectations of an increasingly online population will drive technological change towards the delivery of a digital pathway. The use of such technology as a tool to facilitate the administration of justice, particularly in eTrials is more entrenched than virtual courts such as eCourtroom, which are rare. Nevertheless, the implementation of virtual courtrooms demonstrate that they can provide many advantages when directed to a specific purpose and regulated to protect the security and privacy of personal data. The current application of this technology in many bankruptcy matters illustrates how the selection of a digital pathway can improve access to justice as well as demonstrating the complexity involved in balancing the interests of the debtor, creditor and the public. The use of a virtual court were assessed using two different methods to provide a more comprehensive assessment and methodological triangulation: the first, case studies of matters heard in eCourtroom; and second, qualitative data analysis of responses to a questionnaire by the Registrars of the Federal Court and Federal Circuit Court.

Research that examined the disruptive potential of digital applications provided some interesting insights for the empirical research in this chapter. Conley et al used findings from an empirical study to determine the cause of difference '*in cost of flows* of personal information' between online court records and hard copy records in court houses.[1254] The empirical study involved conducting two systems of online search: the first, using PACER[1255] and Google Scholar; the second, searching at two physical courthouses. The main finding was that there was a significant difference in the cost of retrieval between online and local access.[1256] This was not found to be due to the choice of search medium only but as well to factors such as 'search interfaces, indexing characteristics, and linkages to other information sources'.[1257]

[1254] Conley et al, above n 292, 810.
[1255] PACER, above n 468.
[1256] Conley et al, above n 292, 814.
[1257] Ibid 824.

Conley et al analysed the transition of court records from local to online access found a need to reconcile the 'two strong currents' of openness and privacy.[1258] They found that the debate over the medium for online access has become 'one about core societal values'[1259] of privacy and openness. The impact of placing digital court records online was examined in view of Nissenbaum's theory of contextual interpretation of informational privacy.[1260] They concluded that avoiding new technology is not an option for courts. Courts instead were considered to 'have an obligation to rewrite rules governing the creation of, and access to, public court records'.[1261]

Their policy recommendations for access included three options: the first involved the immediate redaction of all identifying information;[1262] the second, the redaction of identifying information for online documents and retaining the status quo for local,[1263] hard copy access; and the third, a 'fine-grained differential access' which would involve a technological solution by system designer building in the capacity to tag data fields to support differential access.[1264] These options were proposed because it was considered that the radical changes brought by new technologies, specifically enabling court records, which are a repository for useful information about people, to be placed online, made it necessary to 'sustain the underlying interest and values'.[1265]

In the research of Conley et al, the impact of the altered information flows in online access, particularly on the values and purposes internal to courts and the justice system were found to 'increase the hardship of participants in court cases'[1266] and increase difficulties for non-parties, such as witnesses, who have contributed to court proceedings. It was considered that their privacy may be overlooked and possible disclosure of personal data may serve as a disincentive to participate in court proceedings. Hardships, such as harassment, job discrimination, loss of opportunities and the chance of having records expunged were identified as reasons for policy changes in the 'world of open access to full and complete records'.[1267]

To provide more effective digital access to justice in the resolution of disputes, various questions remain to be resolved: how personal data will be protected, which organisations or governments will

[1258] Ibid 774.
[1259] Ibid 775.
[1260] Ibid 803.
[1261] Ibid 777.
[1262] Ibid 839-843.
[1263] Ibid 843-844.
[1264] Ibid 844-845. An example given of this policy option was the use of technical tools with a redaction default for non-party names, members of juries, witnesses, and people inadvertently implicated in a case.
[1265] Ibid 845-847.
[1266] Ibid 837.
[1267] Ibid 837-839.

provide the regulations and what type of regulations will be necessary. As effective as the security procedures[1268] and protocols might be, personal information remains a greater regulatory challenge than originally envisaged in the pre-digital era, once placed in the global digital environment. As Floridi has noted, '[w]e live in a single infosphere, which has no "outside" and where intra- and inter-community relations are more difficult to distinguish'.[1269] It is an infosphere where a person '*is* her or his information' and where the protection of informational privacy is the same as the protection of identity and therefore a 'fundamental and inalienable right'.[1270]

As my research question is a normative question—to what extent *should* the innovative technologies of Web 2.0 be used to enhance access to justice—in the concluding chapter I will address strategies for engagement with Web 2.0 applications. As Conley et al found, the use of Web 2.0 applications has exposed altered patterns of information flow and provided new access options revealing policy ambiguities and undermining 'unexpressed policy expectations, particularly those relating to privacy interests'.[1271] The regulatory framework for the protection of privacy, particularly that relating to the courts' repository of personal data, needs to be revisited to ensure enhancement of access to justice in Australian courts and a resolution of the tension between access and privacy.

[1268] The Federal Court uses SSL V3 certificates by VeriSign, to encrypt information being transmitted through the Internet to the Court's eServices facilities. This encryption prevents the information being viewed or tampered with during transit. Information entered into eLodgment (such as party names and details) is stored on a secure system that has been designed to ensure that loss, misuses, unauthorised access or disclosure, alteration or destruction of this information does not occur. <http://www.fedcourt.gov.au/online-services/elodgment/faqs-technical>.
[1269] Floridi, above n 561, 193.
[1270] Ibid 195.
[1271] Conley et al, above n 292, 829.

Chapter Six – Strategies for enhancing access to justice: resolving the tension

6.1 Introduction

In this chapter I will consider strategies to resolve the tension in the digital environment which will enable Web 2.0 applications to provide access to justice and to protect personal information. This will involve an examination of the regulatory implications of Web 2.0 applications and the extent to which the protection of personal information should be considered in constructing effective strategies for providing access to justice, particularly strategies of relevance for the use of innovative applications by the courts. An examination of the regulatory implications will be set within Floridi's philosophical framework—his ontological interpretation of informational privacy. This framework provides a structure for consideration of the use of digital technologies by linking personal information to personal identity and human dignity.

The use of Web 2.0 applications in the legal system is not just a problem for the future but a more immediate one. The amplification of tension between access and privacy by Web 2.0 technologies is not a development that can be explained simply by the increased capacities and speed of processing, nor the change in quantity and quality of data collected, recorded and managed.[1272] At a more fundamental level it is the transformation of the information environment or infosphere made possible by digital technologies that imposes an imperative on the regulatory environment, an exigent demand for a law and technology theory and data ethics. This is an imperative dictated by the potential for technology to be the regulator, or what can be viewed as the enigmatic relationship between law and technology that Lessig has labelled 'Law Regulating Code Regulating Law'.[1273] This interaction between law and code implies a growing reliance on algorithms to analyse the extensive use of data, much of it personal, and 'the gradual reduction of human involvement or even oversight'[1274] with the resulting consequence for the rule of law.

[1272] Floridi, above n 561, 186.

[1273] Lawrence Lessig, 'Law Regulating Code Regulating Law' (2003) 35 *Layola University Chicago Law Journal* 1-14. Other authors, such as Tim Wu dispute Lessig's assertion about code as law and consider that instead code should be viewed as a mechanism for avoiding and thus shaping law. Furthermore, Wu using an economic compliance model, concluded that code's ability to circumvent regulation can be 'understood as a productive part of the process of law': see Tim Wu, 'When Code Isn't Law' (2003) 89 *Virginia Law Review* 679, 689.

[1274] Luciano Floridi and Mariarosaria Taddeo, 'What is data ethics?' (2016) 374(20160360) *Philosophical Transactions of the Royal Society A* 1-5, 3 <http://dx.doi.org/10.1098/rsta.2016.0360>.

At issue is the extent to which such technologies *should* be used to enhance access to justice. This is dependent on finding a balance between open justice and the protection of privacy, ensuring that access means 'access to justice' not merely open access at the expense of justice, so that access is not 'a limitation on the attainment of the fundamental goal of justice'.[1275]

The complex regulatory environment in which these applications are situated poses significant challenges for their use and for the implementation of effective controls. Elements of this complexity arise from the extent and variety of applications;[1276] the threats to the security of information; the global nature of the Web 2.0;[1277] and the philosophical diversity and ethical pluralism in the digital environment.[1278]

The regulatory environment is characterised by a global information society. As Wu considered, the information itself representing 'an extremely complex phenomenon not fully understood by any branch of learning, yet one of enormous importance to contemporary economics, science, and technology'.[1279] As Floridi found:

> Virtually any of the crucial challenges that we are facing is linked to information and communication technologies, in terms of causes, effects, solutions, scientific investigations, actual improvements, conceptual resources needed to understand them, or even just the wealth required to tackle them … [1280]

By tracing the development of past information empires, Wu found that industries that deal in information are 'naturally and historically different from those based on other commodities.'[1281] He concluded that society today is one dependent on electronic information and, therefore, with everything on the internet, now a 'part of America's basic infrastructure'[1282] in contrast to previous information empires, this time it is different and the

[1275] Smith, above n 304, 17.

[1276] Between 2005 and 2015 the rise of the mobile internet has added to this complexity. The Internet Society Report (2015) reported that by May 2012 there would probably be 3 billion internet users with mobile internet penetration forecast to reach 71% by 2019. Mobile phone service was reported to be available to more than 90% of the global population with new features, such as sharing videos and learning skills being accessed through apps, not browsers. Over 1 million of these apps are available and have been downloaded more than 100 billion times <http://www.internetsociety.org>.

[1277] See Chapter One, discussion about the nature of Web 2.0; see also Chapter Three, discussion of privacy and the global reach of Web 2.0 applications.

[1278] See later discussion in Chapter Three and in this chapter.

[1279] Tim Wu, 'An Introduction to the Law & Economics of Information' (22 March, 2016) Columbia Public Law Research Paper No 14-399, *Columbia Law and Economics Working Paper No 482*.

[1280] Luciano Floridi, 'Turing's three philosophical lessons and the philosophy of information' (2012) 370 *Philosophical Transactions of The Royal Society* 3536, 3539.

[1281] Tim Wu, *The Master Switch: The Rise and Fall of Information Empires* (Atlantic Books, 2010) 6.

[1282] Tim Wu, 'Network Neutrality: Competition, Innovation, and Nondiscriminatory Access', (24 April 2006) <https://ssrn.com/abstract=903118>.

'potential power to control' so much greater.[1283] He supported the view that the protection of consumer choice against market power would be 'a minimum and appropriate role of government.'[1284]

In analysing changes and strategies necessary to regulate Web 2.0 applications for access and privacy, Bennett Moses considered that it is necessary to understand the institutional capacity already in existence.[1285] She examined the role of institutional mechanisms in Australia through which law has been modified as a result of technological change, such as the Productivity Commission, the Copyright Law Review Committee and Royal Commissions which she considered have played an important role in proposing regulatory changes that have responded 'to market failures and inequities requiring intervention.'[1286]

I will examine the necessity for regulating Web 2.0 and the various modalities of control, particularly the future role for the rule of law which is challenged by the use of alternative methods of protection for personal data, whether techno-regulation or techniques such as obfuscation,[1287] self-regulation or imposed market regulation. The legal protection for privacy and its complex relationship to disruptive technologies will be analysed to determine the strategies that will provide a regulatory framework for providing access to justice using disruptive technologies.

6.2 Regulating Web 2.0 applications for access and privacy

6.2.1 Reasons for regulating Web 2.0

Without effective regulation of Web 2.0 applications, access to justice will be denied to those who, despite digital literacy, wish to participate online and are not prepared to pay the price of uncontrolled disclosure of personal information. The tension between the desire to participate in technological innovation and protect the personal and social cost caused by the

[1283] Wu, above n 1281, 318.
[1284] Wu, above n 1282, 7.
[1285] Lyria Bennett Moses, 'How the Law "Copes" with Technological Change' (2011) 20 *Griffith Law Review* 762, 788.
[1286] Ibid, 779.
[1287] Finn Brunton and Helen Nissenbaum, *Obfuscation: A User's Guide for Privacy and Protect* (The MIT Press, 2015). Brunton and Nissenbaum define "obfuscation" as "the deliberate addition of ambiguous, confusing, or misleading information to interfere with surveillance and data collection". It was described as a tool for interfering with search-query logs and has been extended by Brunton and Nissenbaum as "an addition to the privacy toolkit" (97) for responding to privacy threats. The concept's development arose from research into TrackMeNot (<http://c.nyu.edu/trackmenot/> It is a technique that has raised ethical issues and has been seen as adversarial and 'in part, a *troublemaking* strategy' (62) however, its legitimacy has been defended on the basis that it "offers a means of striving for balance defensible when it function to resist domination of the weaker by the stronger. A just society leaves this escape hatch open' (83).

loss of privacy continues to inform the debate about the implementation of new technologies.[1288] A great deal has been written about the death of privacy as a value that cannot exist in the digital world.[1289] Despite its struggle for survival and the acceptance that data collection is a part of modern life, research reveals privacy is valued,[1290] although there remains some difficulty is determining what information people want to protect and at what cost.[1291]

The shifting ethical landscape raises significant philosophical and moral implications with a 'kaleidoscope of lenses'[1292] being necessary in regulatory discussions to accommodate the plurality of ethics within what is largely a 'communicative process'.[1293] The adequacy of the normative framework in which new technologies can be assessed has been suggested by Brownsword as utilitarianism,[1294] deontology[1295] and liberalism, although he recognised that other frameworks may apply.[1296] Floridi has recommended a new branch of ethics[1297] that will study and evaluate moral problems relating to data. This would build on the foundation provided by computer and information ethics while 'shifting the level of abstraction of ethical enquiries, from being information-centric to being data-centric' and would include

[1288] Richard Edelman, *The Power of the Earned Brand'*, (Report, Edelman, 23 June 2015) <http://www.edelman.com>.

[1289] In 1999 Sun Microsystems CEO, Scott McNealy declared there is 'zero privacy'. This was reported by Polly Sprenger, 'Sun on Privacy" "Get Over It" in *Wired* (online) 26 January 1999, when Soctt McNealy was lauching a new technology for Sun Microsystems <https://www.wired.com/1999/01/sun-on-privacy-get-over-it>; other authors include: Reg Whitaker *The End of Privacy: how total surveillance is becoming a reality* (The New Press, 1999); Kieron O'Hara, *The Spy in the Coffee Machine: The End of Privacy as We Know It* (Oneworld Publications, 2008); Simson Garfinkel, *Database Nation: The Death of Privacy in the 21st Century* (O'Reilly Media, 2000).

[1290] European Commission, *Special Eurobarometer 432: Data Protection* (EU Directorate-General for Communication, June 2015). This showed that the protection of personal data remains a very important concern for citizens and only a minority consider they have complete control over the information they provide online. Although a large majority find that providing personal information online that they accept it is an increasing part of modern life and there is no alternative if they require the services. A majority of people considered that their explicit approval should be required for the collection and processing of data. Only 18% fully read privacy statements. Nine out of ten Europeans considered that it is important for them to have the same rights and protections over their personal information, regardless of the country in which the public authority or private company offering the service is based <http://ec.europa.eu/public_opinion/index_en.htm>.

[1291] See discussion in Chapter Three of this thesis.

[1292] Julia Black, 'Regulatory Conversations' (2002) 29 *Journal of Law and Society* 163-196, 163.

[1293] Ibid 164.

[1294] Utilitarianism – this is often referred to as consequentialism because it is a theory of normative ethics that views a moral action as one that dependent on the consequences rather than the inherent character or motive. It involves a weighing up of the cost of achieving a benefit with the improvements. The most influential contributors were Jeremy Bentham and John Stuart Mill.

[1295] Deontology – This is an ethical view that focuses on the morality of the actions themselves, not the consequences and is based on the action's adherence to a rule. It appeals to human dignity. The most influential philosopher was Immanuel Kant.

[1296] Liberalism – this focuses on the individual in a society where free choices are available. It supports a human rights basis for regulation.

[1297] Floridi and Taddeo, above n 1274, 374.

computational operations and algorithms. While Floridi acknowledges the 'shift from *information* ethics to *data* ethics is probably more semantic than conceptual',[1298] the shift does recognise that it is not the computers and Web 2.0 applications that are the problem but what they do with the data, in particular the ethical problems with issues such as privacy.

Despite the difficulties of assessing the relevant ethical landscape, there is considerable support for governance policies and architecture which would promote open and public spaces on the internet and protect human rights such as privacy.[1299] The internet has been viewed as a 'key element for the enjoyment and the promotion of human rights', a global resource and, as such, 'appropriate Internet governance' has been recognized as supporting 'the right of everyone to have access to and use information and communication technologies in self-determined and empowering ways'.[1300]

While the use of Web 2.0 has been considered necessary to ensure access to services, information and markets, regulation has also been seen as a way of ensuring protection for human rights such as privacy and freedom of speech. The issue that I will consider is the various modalities of control to determine which regulatory environment would promote both access and privacy.

6.2.2 Conflicting modalities of control

Of the four modalities of control discussed by Lessig – markets, law, norms and architecture or code – code was seen as the modality most requiring focus for regulation in the future.[1301] However, concerns about the role of law in regulating the digital environment has also been raised by authors such as Brownsword, Koops and Hildebrandt.[1302] The role of markets has demonstrated an inherent incompatibility with privacy due to the value of online data and consequently there has been reluctance by governments and private companies to provide privacy protection. The conflict between balancing economic demands and protecting privacy can be illustrated in the US by the proposal from Senator Elizabeth Warren to the Federal

[1298] Ibid 3.
[1299] Farida Shaheed, 'Internet governance must ensure access for everyone – UN expert'. *UN News Centre* (online) (May 2012). Shaheed, the Special Rappporteur in the field of cultural rights in the United Nations Office of the High Commission for Human Rights, considered the internet a global resource news report <http://www.un.org/apps/news/story.asp?NewsID=42039#.V7ZtDnkcScw>.
[1300] Ibid.
[1301] Lessig, above n 83.
[1302] Mireille Hildebrandt, *Smart Technologies and the End(s) of Law; Novel Entanglements of Law and Technology* (Edward Elgar Publishing, 2015).

Communications Commission (FCC) to adopt strong consumer privacy rules for internet service providers (ISPs).[1303] This was primarily to protect low-income consumers whom she considered were easily exploited by companies marketing products.

Online norms have been shown to fluctuate. This has been demonstrated in OSNs, where despite self-disclosure of private information, expectations of privacy have remained. Therefore, norms alone have been unable to provide consistency. A more detailed discussion of the evolving nature of privacy, has been presented earlier,[1304] however privacy presents an exceptional challenge for regulation as the societal norms of privacy are characterised by contradiction, change and flux as people race to connect and interact online yet report sensitivity to disclosure of personal information. The protection of personal information is informative of the tensions between the modalities of control.

Law and code have become the focus of regulatory discussion, separately and in conjunction with each other. As Hildebrandt has argued, 'without legal protection by design we face the end of law as we know it'.[1305] The legal protection by design that she advocates is seen as conceptually different from 'techno-regulation' because it is 'compatible with enacted law', it 'can be resisted' and it may be contested in court providing legal certainty and justice due to being 'visible' and 'contestable'.[1306]

The signals[1307] that constitute this complex technological environment impact on the way regulatees behave. Research on the governance of biotechnologies has found that '[o]nce the modality moves away from law and social norms, to market, architecture and code, the signal

[1303] In a letter dated 21 June 2016 to the Chairman of the FCC, Senator Warren supported the establishment of clear consumer privacy standards for broadband internet access service (BIAS) because she considered that internet access is an essential service and that to access the internet 'consumers have no choice but to disclose personal information'. Senator Warren considered that the FCC should 'ban unreasonable practices that coerce low-income consumer into giving up their privacy in return for access to basic internet services', especially as BIAS providers develop 'new invasive and abusive practices' for using personal data. She gave as an example the practice of AT&T's Gigapower Internet service requirement that consumers pay as much as an additional $66 a month for the service to protect their privacy and the boast by the CEO of Cable One that his company uses subscriber's personal data to run credit check on them and then offer lower-quality customer service to those with low credit scores, <https://www.warren.senate.gov>.

[1304] See Chapter Three of this thesis.

[1305] Hildebrandt, above n 1294, 214.

[1306] Ibid 214-219.

[1307] R Brownsword, 'Regulating, Biobanks: Another Triple Bottom Line', Chapter 3 in Giovanni Piscuzzi, Umberto Izzo and Matteo Macilotti (eds) *Comparative issues in Governance of Research Biobanks: Property, Privacy, Intellectual Property, and the Role of Technology* (Springer, 2013). Brownsword refers to the regulatory environment consisting of 'signals and steering mechanisms, that are intended to direct the actions, transactions, and interactions of regulatees', 54.

to regulate can take on a different non-normative, character …'[1308] It has been alleged, in relation to biobanks[1309], that 'technology may change the contents of protected legal interests' from a 'right to be let alone' to the 'right of controlling the information' or 'informational self-determination'.[1310] Once non-normative signals gain importance, the values of legality and the rule of law may fade, particularly where behaviour is limited by designs in the technology itself.

The regulation in such areas of biotechnology has importance lessons for information technology and law. The need for regulation has been regarded as more urgent in biotechnology, and the use of new technologies for research more advanced than the use of Web 2.0 applications in law. Biobanks in Europe have been regulated with a 'clear political and legal commitment to respect human rights', providing free and informed consent, privacy, fair data processing and proprietary rights where appropriate so that the regulatory environment is 'not so reliant on coding, design, and technical fixes that the conditions and context for moral community are compromised'.[1311] A clear political and legal commitment to respect personal information within the global digital environment, as found in biotechnology, could form a template for future regulation. There would be a greater opportunity for implementation of Web 2.0 application once a greater awareness was created of the possibilities of privacy protection.

6.3 A role for law in the conflicting modalities of control online

6.3.1 Conceptual gap between law and innovation?

The use of code to regulate the flow of personal information has been considered by some policymakers as a tool to embed privacy as an integral part of the design of a technological system and to offer ex ante protection. However, Birnhack, Toch and Hadat found, in analysing the mindset of privacy and technology, that 'the discursive and conceptual gap between law and technology'[1312] form a major obstacle to the implementation of effective

[1308] Giovanni Piscuzzi, Umberto Izzo and Matteo Macilotti (eds) *Comparative issues in Governance of Research Biobanks: Property, Privacy, Intellectual Property, and the Role of Technology* (Springer, 2013) 44.
[1309] Biobanks became important from the 1990s for the storage of biological samples, particularly human tissue research such as genomics.
[1310] Piscuzzi, Izzo and Maalotti (eds), above n 1300, 2.
[1311] Roger Brownsword in Chapter 3 'Regulating Biobanks: Another Triple Bottom Line' in Giovanni Piscuzzi, Umberto Izzo and Matteo Maalotti (eds) *Comparative issues in Governance of Research Biobanks: Property, Privacy, Intellectual Property, and the Role of Technology* (Springer, 2013) 41.
[1312] Michael Birnhack, Eran Toch and Irit Hadar, 'Privacy Mindset, Technological Mindset' (2014) 55 *Jurimetrics: Journal of Law, Science & Technology* 55-114, 55.

protection of privacy because they regulate the flow of information in totally different ways, with different goals and different constraints.

Rules embedded in code lack transparency and accountability. Code has been viewed as suffering from a 'democratic deficit'.[1313] It is regulation that has been developed 'in the laboratories of corporations', particularly companies such as Facebook, Twitter and Google that exert considerable control over personal data and where the 'data warehousing mindset'[1314] is at odds with data minimization.[1315] Koops and Leens did not consider that privacy regulation can be coded, and rejected the suggestion that the 'privacy by design'[1316] provisions in data-protection legislation can work alone. They should be viewed instead as part of general "'communication" strategies'.[1317] This is because they consider that embedding data protection requirements in system software is not the only interpretation of 'privacy by design' but such a concept extends to 'fostering the right mindset' for those responsible for the development and running of data processing systems not just meaning 'rule compliance by techno-regulation'. Privacy by design is viewed as a paradigm building on previous ideas such as 'value-sensitive design',[1318] 'code as law'[1319] and PETs.[1320]

[1313] Leenes and Koops, above n 218, 330.

[1314] Birnhack, Toch and Hadar, above n 1290, 51. 'Data warehousing is an engineering field that focuses on collecting, integrating, and analyzing large quantities of data from heterogeneous sources over longitudinal periods of time. Data science is an emerging field and applies sophisticated algorithms to mine big datasets, find patterns, and use them to predict behavior. Data science builds on data warehousing, data mining, and other practices related to collecting, managing, and analyzing data, form small to large scale datasets (commonly known as big data) …large corporations almost necessarily have a data warehouse in place. These organizations collect data about their customers and hence raise issues of informational privacy.'

[1315] Article 6.1(b) and (c) of the European Union Directive 95/46/EC and Article 4.1(b) and (c) of Regulation EC (No) 45/2001 provide that personal data must be 'collected for specified, explicit and legitimate purposes and be 'adequate, relevant and not excessive in relation to the purposes for which they are and/or further processed'.

[1316] Privacy by design and privacy by default has been introduced as one of the main principles of the new legal framework for the protection of personal data by the EU Commission to ensure that the security requirements are introduced at the initial stages of development of technology. Article 23 of the Data Protection proposal 9565/15 provides for data protection by design and by default. This article proposes that 'controllers shall implement (…) technical and organizational measures appropriate to the processing activity being carried out and its objectives, such as data minimization and pseudonymisation…' The proposal for a General Data Protection Regulation (5853/12) was adopted on 25 January 2012 with the intention to replace Directive 95/46/EC.

[1317] Bert-Jaap Koops and Ronald Leenes, 'Privacy regulation cannot be hardcoded. A critical comment on the "privacy by design" provision in data-protection law' (2014) 28 *International Review of Law, Computers & Technology* 159.

[1318] The value-sensitive design project emerged in the 1990s as an approach to the design of information and computer systems that accounts for human values such as privacy and human dignity as well as usability and conventions in computer systems. The project is based on interactions between technical structures and individuals, groups and institutions with an understanding that "expectations, conventions, institutional practices, policies, laws and regulations push back on the technology – shaping and constraining its use, prodding and creating opportunities for new technical developments" <http://vsdesign.org>.

[1319] Lessig, above n 83. See discussion of Lawrence Lessig's 'code' theory in this thesis, 17-20:

It has even been suggested that peer-to-peer technologies[1321] could be used to assist the evolution of law as a regulatory system.[1322] Traditionally peer-to-peer technologies have been disruptive, distributed architectures making the enforcement of law, particularly copyright law, difficult.[1323] Legal regulation has aimed at controlling peer-to-peer technologies to prevent copyright infringement and criminal activity[1324] and in so doing it has controlled legitimate activities. They have been used to preserve privacy, but at the same time, also used to escape legal control and censorship. De Rosnay's proposal is for a new paradigm of integration and conceptual relationships where community rights and duties are recognised rather than individual rights.

At the more extreme end of the technological spectrum, government agencies have used automated decision-making which raises issues of transparency, accountability, the role of the rule of law, and ultimately the concern of a development towards an 'algorithmic society'[1325] and the dominance of artificial intelligence[1326] as matters of urgency. Caution has been recommended in the use of automated decision-making in government agencies made

[1320] A comprehensive analysis of privacy-enhancing technologies, such as: privacy policy languages, anonymity techniques, authentication and identity management, authorization and access control, usable security and privacy mechanisms, as well as a useful chart of the hierarchy of potential privacy constraints (204) can be found in: Yang Wang, 'Privacy-Enhancing Technologies', Chapter 13M Gupta and R Sharman (eds) *Handbook of Research on Social and Organizational Liabilities in Information Security"* (2008) Hershey, PA.

[1321] Tor is an example of peer-to-peer technology that promises privacy protection and anonymity by providing free software which bounces 'communications around a distributed network of relays run by volunteer all around the world'. This is to prevent network surveillance and which prevents the sites visited discovering the physical presence of the computer <https://www.torproject.org>.

[1322] Melanie Dulong de Rosnay, 'Peer-to-peer as a design principle for law: distribute the law' (online) January 2015, 6 *Journal of Peer Production* <http://peerproduction.net/issues/issu-6-disruption-and-the-law>

[1323] *Universal Music Australia Pty Ltd v Sharman License Holdings Ltd* (2005) 222 FCR 465. In this case the applicants claimed copyright in various sound recordings and claimed that the respondents had authorized the users of Kazaa Software to infringe the applicants' copyright. Kazaa software enabled users to share the recordings, whether subject to copyright or not, via a peer-to-peer file-sharing system. The claim succeeded against six of the respondents; see also *Roadshow Films Pty Ltd v iiNet Limited (No 2)* (2012) 248 CLR 42 where the High Court of Australia found copyright infringement by the use of the BitTorrent system which allowed films to be shared using a peer-to-peer system.

[1324] de Rosnay, above n 1300.

[1325] The 'paradigm of the algorithmic society' has been viewed as one 'bound up in the unknown': see Marina Bradbury, 'There's an algorithm for that. Or there soon will be' *OECD Insights* (online) 18 May 2016. It reflects a view that 'algorithms, somehow mysterious and inevitable, are contributing to the shape of our lives both big and small': see Paul Dourish, 'Algorithms and their others: Algorithmic culture in context' (online) July-December 2016 *Big Data & Society* 1-11, 1. Dourish discussed the different types of algorithms and distinguished the social analysis of algorithms, particularly the problems presented by opaque algorithms and accountability.

[1326] Despite the concern amongst some lawyers of control by AI, philosophers such as John Searle and Luciano Floridi dispute the existence of AI. They distinguish the syntactical capacity of machines, such as computers, from the distinguishing feature of the human brain and its semantic abilities which makes cognitive functioning possible: John Searle and Luciano Floridi, 'Discussion on Artificial Intelligence' (online) presented at the conference *Technology and the Human Future*, 21 October 2016, Oslo <https://www.youtube.com/watch?v=b6o_7HeowY8>.

possible by advances in technology. Rule based systems,[1327] used to assess eligibility for tax returns and social security payments, while introducing efficiencies can also include programming errors and thereby errors in final decisions without 'vigilance in ensuring that compulsive powers are conferred and exercised in a manner consistent with fundamental administrative law values'.[1328] Such technology increases non-normative signals, such as economic efficiency gains at the expense of legal, normative signals. Rubinstein examined how embedded technology was designed to direct compliance of behaviour in line with regulatory norms.[1329] Bamberger considered that 'the reality is even more complicated, muddled, and less differentiated than these original important dichotomies suggest'.[1330] He viewed the code of technology as more than an extra mode of regulation and as 'part and parcel of management and decision making, of action and inaction'.[1331]

Justice Kirby considered that there existed a dilemma, in that failing to provide law to manage technology, this could also be making a decision. He also recognised that there can be a problem in acting prematurely and passing laws that 'place a needless impediment upon local scientists and technologists'.[1332] As well, to act too quickly and pass laws that are ignored or are ineffective can also be a problem, a 'contradiction or tension, difficult to resolve'.[1333] Lessig similarly recognised that the failure to regulate can have 'perverse consequences', finding that the failure to regulate can increase the demand for private regulation.[1334] In discussing another paradox, Kirby referred to the conflict presented by Lessig, between First Amendment values and the current state of American copyright law.[1335] The relevance of this dilemma was found in the global impact of laws such as the incorporation of US copyright law through the code of purchased software and products. The 'democratic deficit' of technology was seen as deriving from the way technology both enhances and diminishes democratic

[1327] Justice M Perry and Alexander Smith, 'iDecide: the legal implications of automated decision-making', (Paper delivered at the Cambridge Centre for Public Law Conference 2014: Process and Substance in Public Law, University of Cambridge, 15-17 September 2014).
[1328] Melissa Perry, 'Administrative Justice and the Rule of Law: Key Values in the Digital Era' , (paper presented at the Rule of Law in Australia Conference, The Rule of Law, the Courts and Constitutions, Intercontinental Hotel, Sydney, 6 November 2010) 9.
[1329] Ira S Rubinstein, 'Regulating Privacy by Design' (2011) 26 *Berkeley Technology Law Journal* 1409.
[1330] Kenneth A Bamberger, 'Foreword: Technology's Transformation of the Regulatory Endeavor' (2011) 26 *Berkeley Technology Law Journal* 1315.
[1331] Ibid 1315.
[1332] Kirby, above n 73, 20.
[1333] Ibid 22.
[1334] Lessig, above n 1273.
[1335] Kirby, above n 73, 26.

governance[1336] because, while the distribution of information has been revolutionised, the quantity of information has allowed 'its manipulation and presentation in a way "antithetical to real democratic accountability" and concentrating power in an unimaginable manner'.[1337] Kirby asked whether, '[g]iven the importance of technology to the current age, how do we render those who design, install and enforce such programmes accountable to the democratic values of our society?',[1338] ensuring there is a role for data ethics in regulation.[1339]

In order to assess the role of law in the digital regulatory environment, I will examine the different developments in Australia, the UK, the US and EU to assess the effectiveness of law in protecting personal information in the digital era and suggest strategies to assist the future use of innovative Web 2.0 applications.

6.3.2 The role of law in protecting privacy in Australia

The legal protection of privacy in Australia has been characterised by uncertainty and incremental changes as technology developed. A number of reports recommending reform[1340] and the introduction of technologies have lauded new technologies as increasing access to justice and efficiencies. Recently the Hon Michael Kirby, speaking at the launch of Privacy Awareness Week in May 2016, argued for an urgent need to provide better protection for privacy in Australia.[1341]

In Australia the right to privacy has not been recognized by the common law. This tort was rejected in 1937 in *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor (Victoria Park).* [1342]

[1336] Ibid 27.
[1337] Ibid 28.
[1338] Ibid 29.
[1339] Floridi and Taddeo, above n 1274, 1-5. These authors discuss the development of a new branch of ethics with studies and evaluates the moral problems related to data, concentrating on the content and nature of computational operations –the interactions between hardware, software and data rather than on the variety of digital technologies.
[1340] Australian Law Reform Commission (ALRC), *Unfair Publication: Defamation and Privacy,* Report 11 (1979); ALRC, *Privacy*, Report 22 (1983); ALRC, *For Your Information: Australian Privacy Law and Practice,* Report 108 (2009); NSW Law Reform Commission, *Invasion of Privacy*, Report 120 (2009); Victorian Law Reform Commission, *Surveillance in Public Places*, Report; South Australian Law Reform Institute, *Too Much Information: A Statutory Cause of Action for Invasion of Privacy,* Issues Paper 4 (2013).
[1341] Stefanie Garber, 'Kirby backs "long overdue" NSW privacy reform (6 May 2016) *Lawyersweekly* <http://www.lawyersweekly.com.au>
[1342] *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor (Victoria Park)* (1937) 58 CLR 479 – in this case an elevated platform was erected on land adjoining a racecourse. The owner allowed an employee of a broadcasting company to use the platform during race meetings to describe the races and announce the results which could be read from notice boards. While it was found that it may be desirable that there be some limitation of invasion of privacy, Latham CJ found that 'no authority was cited which shows that any general right of privacy exists', 496.

However, in *Grosse v Purvis* the District Court of Queensland took a contrary view. [1343] Chief Justice Gleeson in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd*[1344] referred to two reasons for caution in recognising a new tort of privacy; the lack of precision in the concept of privacy and the 'tension' between free speech and privacy.[1345] Justices Gummow and Hayne commented[1346] that at least one or more of the four invasions of privacy referred to in this case would be actionable under recognized causes of action such as, injurious falsehood, defamation, confidential information and trade secrets, passing-off, the tort of conspiracy and nuisance. In this comment the judges were acknowledging the effectiveness of a reductionist view of privacy.[1347]

Both Gummow and Hayne JJ in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* agreed that the decision in *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor*[1348] 'does not stand in the path of the development' of an enforceable right to privacy, although, privacy was not at the forefront of the arguments by the plaintiff in *Victoria Park*.[1349] It was considered that whatever development may occur in the area of privacy law it would not benefit a statutory or artificial person, only a natural person.[1350] Whether it would be appropriate for the High Court to declare 'invasion of privacy' as an actionable wrong was considered difficult by Justice Kirby[1351] and a question to be postponed in the circumstances

[1343] In *Grosse v Purvis* [2003] QDC 151 the District Court of Queensland the tort of privacy was recognized and in *Doe v Australian Broadcasting Corporation* [2007] VCC 281 by the Country Court of Victoria, however both cases were settled before appeals and no appellate court has confirmed the existence of this tort.

[1344] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199. In this case the factory, Lenah Game Meats processed brush-tail possums for export, mainly to Asian countries. Access to the factory was obtained by an unknown person and cameras installed which filmed sensitive parts of the process. The film was retrieved and it was offered to the Australian Broadcasting Corporation for broadcasting. A segment of the film was shown during the ABC 7.30 Report. An interlocutory injunction to prevent this broadcast was unsuccessful before the primary judge (unreported, Supreme Court of Tasmania, Underwood J, 3 May 1999) but succeeded before the Full Court (*Lenah Game Meats Pty Ltd v Australian Broadcasting Corporation* [1999] TASSC 114. Special leave to appeal to the High Court of Australia was granted and the issue of privacy considered. The majority (Gleeson CJ, Gaudron, Gummow, Kirby and Hayne JJ allowed the appeal; Callinan J dissenting).

[1345] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 225-226 [41].

[1346] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199, 255 [123].

[1347] See discussion in Chapter Three of this thesis, 3.4.3 'A reductionist view of privacy?'

[1348] *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479.

[1349] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 119, 250 [111].

[1350] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 119, 258 [132].

[1351] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 119, 277 [187], Justice Kirby referred to the absence of recognition by Australian law reform bodies of an enforceable general right to privacy. The report of the Australian Law Reform Commission in 1983 concluded that "a general statutory right to privacy, as had been enacted in some places overseas, should not be recommended in Australia" and recommended instead that legislation should be specific, defining the values protected and the defences available. His Honour considered [189] in *Lenah Game Meats* that it was not necessary, in the circumstances of this case to decide whether the tort of privacy existed.

of this particular case[1352], particularly as the respondent was a corporation. Justice Callinan commented[1353] that '[p]eople in our society, rightly, expect that their homes, offices and factories will not be broken into with impunity', however whether a right to privacy exists and the principles of such an Australian tort would need to be 'worked out on a case by case basis in a distinctly Australian context' with a balance being sought between 'the value of free speech and publication in the public interest' and privacy. His Honour recognized that the tort based on the right to privacy had developed in the US where it is a complex of four torts and was evolving as it responded to encroachments by the media and others.[1354]

In addition to judicial decisions concerning privacy protection and whether a separate tort is necessary, the literature also reveals continued debate over whether there is any value in introducing a separate tort. Taylor and Wright[1355] considered that following the decision in *Lenah Game Meats* Australian courts appeared to have reverted to a more conservative approach to privacy, compared to the US and Canada and moved away from the development of a tort of privacy.

Stewart[1356] concluded that *Lenah Game Meats* raised more questions than it answered[1357] and the role for a tort of privacy remained unclear.[1358] He considered that a clearer expression of the interests to be protected as private and 'a discussion of the relationship between privacy, property and confidentiality' would be required. Stewart predicted that property rights would remain important in the protection of privacy. To determine what would be protected as private it would be important to determine the 'interplay between the way in which information is obtained and the extent to which that is evident to third parties in receipt of the information, the damage done in release of the information and the benefits to be derived from use or disclosure of the information'.[1359]

[1352] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 119, 278 [189].
[1353] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 119, 327 [329].
[1354] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 119, 325 [323].
[1355] Greg Taylor and David Wright, '*Australian Broadcasting Corporation v Lenah Game Meats:* Privacy, Injunctions and Possums: An analysis of the High Court's Decision' (2002) 26 *Melbourne University Law Review* 707-736.
[1356] Daniel Stewart, 'Protecting Privacy, Property, and Possums: *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2002) 30 *Federal Law Review* 177, 201.
[1357] Ibid.
[1358] Ibid 177.
[1359] Ibid 201.

Lindsay,[1360] however, has argued that following the decision in *Lenah* the most obvious way of solving the inadequate protection of personal privacy was either to introduce a tort of privacy or extend the current action for breach of confidence. The choice supported by Lindsay was the tort of privacy because he considered privacy to be conceptually distinct and best protected by specific laws. The extension of breach of confidence was not preferred because of the possibility this 'may result in an unprincipled development of confidentiality law'. Lindsay considered that divergent views in *Lenah* were 'playing possum' by suggesting how the law may develop but not expressing 'settled views', leaving the law unclear.[1361]

Pelletier and Polden presented an interesting juxtaposition of views on whether a new tort of privacy should be introduced, highlighting some of the complexities involved.[1362] Pelletier considered that people should be able to sue when their privacy has been seriously invaded because, without such statutory protection, privacy protection would remain 'piecemeal' and 'of uncertain scope and dubious enforceability'.[1363] He supported statutory reform in preference to the development of the common law to provide certainty and a role for the courts in balancing the right of privacy against the public interest. Polden, however, considered that to introduce a tort of privacy would 'simply introduce another level of complexity, without doing anything to address the existing maze of de facto privacy laws' and it would provide a fertile area for litigation.[1364] He also stressed that another danger would be the potential for undermining existing defamation defences thereby making 'effective defence of robust journalism more costly' and to introduce a right to privacy 'without a co-relative right to freedom of expression' would get the balance wrong.[1365] He contrasted Australian laws with the US where reliance could be placed on the First Amendment to the Constitution which he considered acted as a 'brake on privacy torts'.[1366]

Williams supported the introduction of a tort of privacy in Australia as protection against corporate interest, particularly through social media and to provide a remedy and a deterrent

[1360] David Lindsay, 'Playing Possum? Privacy, Freedom of Speech and the Media Following *ABC v Lenah Game Meats Pty Ltd* Part 11: The Future of Australian Privacy and Free Speech Law, and Implications for the Media (2002) 7 *Media & Arts Law Review* 161.
[1361] Ibid.
[1362] Robert Pelletier, 'A New Tort of Privacy: We should be able to sue' (December 2008) 46 *Law Society Journal* 58-63; Mark Polden, 'Privacy sounds good, but …' (December 2008) 46 *Law Society Journal* 59-63.
[1363] Robert Pelletier, 'A New Tort of Privacy: We should be able to sue' (December 2008) 46 *Law Society Journal* 58-63, 63.
[1364] Mark Polden, 'Privacy sounds good, but …' (December 2008) 46 *Law Society Journal* 59-63, 61.
[1365] Ibid 63.
[1366] Ibid 61.

when personal information and financial details are exposed by businesses or people for commercial gain or negligence.[1367] Williams considered that the Australian government has missed several opportunities, following a number of law reform reports, particularly the two year examination of privacy by the ALRC in 2008. The announcement on 12 March 2013[1368] of another inquiry into privacy was, he considered, merely an indication of indecision. He stated that the issue should not be left to the courts because Parliament would be better able to introduce a tort which paid adequate regard to principles such as freedom of speech.

In Australia the development of protection for privacy has been slow and uncertain. Limited, specific statutory protection for privacy was introduced by the *Privacy Act 1988* (Cth) which protects personal information held by federal government agencies and parts of the private sector. Most Australian States[1369] and Territories[1370]also have privacy legislation directed mainly at the public sector. It is an Act which has been extensively amended, especially in 1990 to apply to the credit reporting industry and in 2000 to apply to the private sector.

In May 2008 an extensive report on privacy law[1371] was finalised by the ALRC.[1372] The right to privacy was recognised, but not as an absolute right. The Report found that privacy must be

[1367] George Williams 'privacy: the fix should not be left to judges' *The Sydney Morning Herald* March 26, 2013.

[1368] Media release: 'Government response to Convergence Review and Finkelstein Inquiry' Senator the Hon Stephen Conroy stated that "The Privacy Tort will be referred to the Australian Law Reform Commission for detailed examination." (12 March 2013)

[1369] In Western Australia there is no privacy legislation that deals with information privacy in the public sector. The *Information Privacy Bill 2007* (WA) was introduced to Western Australia's Parliament on 28 March 2007 but as yet has not been passed. Limited privacy protection is provided by legislation such as the *Freedom of Information Act 1992* (WA) and the *State Records Act 2000* (WA). South Australia also does not have privacy legislation and relies on the Privacy Committee to implement information privacy principles in the public sector. The most comprehensive legislation is to be found in New South Wales and Victoria. The *Privacy and Personal Information Protection Act 1998* (NSW) and the *Health Records and Information Privacy Act 2002* (NSW) regulate information privacy in public sector agencies. In Victoria the *Information Privacy Act 2000* (Vic) and the *Health Records Act 2001*(Vic) provide comprehensive privacy principles. As well the *Charter of Human Right and Responsibilities Act 2006* (Vic) recognizes a right to privacy. The *Personal Information Protection Act 2004* (Tas) provides privacy guidelines mainly directed at the public sector in Tasmania. This is supported by provisions in the *Charter of Health Rights* (developed under s 17 of the *Health Complaint Act 1995*(Tas)) and the *Right to Information Act 2009* (Tas). Protection for personal information is provided in Queensland by the *Information Privacy Act 2009* (Qld).

[1370] A right to privacy was recognized by the *Human Rights Act 2004* (ACT) in the ACT. Specific privacy protection in the ACT is provided by the *Health Records (Privacy and Access) Act 1997* (ACT) and the *Listening Devices Act 1992* (ACT). In the Northern Territory, information privacy in the public sector is protected by the *Information Act 2002* (NT) which contains privacy principles similar to the federal *Privacy Act.*

[1371] 'For Your Information: Australian Privacy Law and Practice', ALRC Report 108, May 2008, Commonwealth of Australia. This followed a 28 month inquiry and resulted in 295 recommendations for reform.

[1372] Ibid. The recommendations aimed at simplification of the *Privacy Act* and related legislation; the development of a single set of Privacy Principles; accountability for cross-border data flow; rationalisation of exemptions; strengthening of the Privacy Commissioner's complain handling procedures; more comprehensive credit reporting; new health privacy regulations; education of young people about the use of their personal information online; notification of data breaches; and the provision of a private cause of action for serious invasion of privacy.

balanced with rights such as freedom of speech and national security. In October 2009 the Australian Government addressed many of the recommendations of this report. The Issues Paper, *A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy*,[1373] in 2011 commented on the current state of the right to privacy in Australian law:

> There is currently no statutory action for invasion of privacy in any Australian jurisdiction, and there is scant common law, with no appellate court recognizing a tort of invasion of privacy.[1374]

The Issues Paper sought views on 'whether the Australian Government should create a right for individuals to seek redress from another person who seriously invades their privacy', the circumstances in which the right should apply and the type of remedies to be made available.[1375] The paper also considered whether current privacy laws were adequate to protect personal data. It identified some key technological developments which have changed the context for the protection of privacy in Australia. These include: greater access to technology, increased connection to the internet, faster internet speeds; the increased level of online participation and the expansion of social networks, blogs and wikis which encourage 'greater levels of engagement and interactivity' as well as the publication of a much greater volume of data. As well, the improvement in accessibility and affordability of technology, including the high rate of mobile phone ownership in Australia were seen as making personal intrusion pervasive. Despite these reservations, technology was viewed in the Report as integral to 'engagement with government, business and each other'.[1376]

In discussing the future direction for privacy legislation in Australia, McDonald noted the impact that the introduction of a statutory action for breach of privacy would make.[1377] She pointed to an awareness that 'the internet and social media have undermined the ability of any government anywhere in the world to create effective and complete legal protection' for

[1373] Australian Government, 'A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy', Issues Paper (23 September 2011) <https://www.ag.gov.au/Consultations/Pages/Righttosueforseriousinvasionofpersonalprivacyissuespaper.aspx> .

[1374] Ibid.

[1375] Ibid, 12

[1376] Ibid, 11.

[1377] Barbara McDonald: 'A statutory action for breach of privacy: Would it make a (beneficial) difference?' (2013) 36 *Australian Bar Review* 241 and Chapter 4, p 63, 'Tort's Role in Protecting Privacy: Current and Future Directions' Simone Degeling, James Edelman and James Goudkamp (eds) *Torts in Commercial Law*, (Lawbook 2011).

privacy[1378] due to the 'largely uncontrollable and often undetectable ability of individuals to spread information and rumour' rather than the activities of media defendants.[1379] She concluded that a 'uniform and carefully targeted statutory action with carefully drafted requirements' would be preferable to an 'ill-defined' statutory action that could be a 'multi-headed monster' with privacy remaining incomprehensively defined. A case-by-case analysis by the courts providing an incremental development of the common law was considered to be a preferable alternative.[1380] It was found that clear guidance about the form and content of a proposed statutory action was not provided in the most recent law reform commission reports[1381] in Australia.[1382]

The ALRC and New South Wales Law Reform Commission (NSWLRC) reports proposed a single cause of action for privacy while in Victoria the proposal was for two causes of action.[1383] An important issue of divergence between the reports was found in whether public interest should be a defence to be established or a balancing consideration. McDonald considered that in an open and democratic society for those who value a 'vigorous press and media' the balancing of public interest is vital and any disclosure of private information should not be actionable unless it is established that there is no 'legitimate public interest in the information'. It is an approach necessary under the European Convention and in the UK following the *Human Rights Act 1998* and should be preferred to the recommendations of the ALRC and NSWLRC where public interest is a defence.[1384]

A legislative remedy for serious invasions of privacy in Australia was strongly endorsed by the Australian Privacy Foundation.[1385] The submission considered that such a cause of action 'would not inhibit effective law enforcement or national security activity' or 'implied freedom of political communication', nor was it thought that the tort would 'burden the legal system

[1378] Ibid 242.
[1379] Ibid 242.
[1380] Ibid 269.
[1381] The Australian federal and state law reform commissions referred to included: The Australian Law Reform Commission (ALRC) *Report 11: Unfair Publication: Defamation and Privacy* (1979); the ALRC *Report 22: Privacy* (1983); the ALRC *Report 108: For Your Information: Australian Privacy Law and Practice* (2008); the New South Wales Law Reform Commission Report 120: *Invasion of Privacy;* and the Victorian Law Reform Commissions Final Report 18: *Surveillance in Public Places*. Barbara McDonald 254 – 257.
[1382] Barbara McDonald, 'A statutory action for breach of privacy: Would it make a (beneficial) difference?' (2013) 36 *Australian Bar Review* 241, 254.
[1383] Ibid 263.
[1384] Ibid 268.
[1385] Bruce Arnold et al, Submission of the Australian Privacy Foundation to the Australian Law Reform Commission, 15 November 2013.

with inappropriate litigation'.[1386] The authors considered that the tort would provide an effective remedy and coherence in Australian jurisdictions, while filling 'a long-standing gap in the common law'.[1387]

The Office of the Australian Information Commissioner (OAIC) has adopted a voluntary compliance approach to privacy regulation and works to ensure the adoption of best privacy practice and the prevention of privacy breaches.[1388] Powers and functions to ensure the protection of personal information have been conferred on the Privacy Commissioner by the *Privacy Act* and other legislation. The OAIC ensures compliance with the obligations of the *Privacy Act*, increased public knowledge of those obligations, assists entities to adopt best practice methods, deters conduct that contravenes privacy obligations and secures appropriate remedies where privacy has been contravened. Where there is a shared interest in addressing privacy issues in foreign jurisdictions, the OAIC seeks to cooperate with privacy regulators in foreign jurisdictions.

The gaps remaining for the protection of privacy can be illustrated by the special case of genetic privacy.[1389] The global nature limits regulatory effectiveness because Australian consumers are able to purchase genetic tests online from companies which could be located in the US, Europe or in other countries. The authors suggest that it is possible that '[i]nternationally harmonized sui generis genetic privacy protection' would be the only effective solution.[1390]

Considering the diverse requirements and business models of industry as well as the diverse consumer needs, 'principles-based law' was chosen as the best regulatory model for privacy protection by the Australian Government. It does not deal with detailed operational requirements but 'sets out high level obligations' to provide maximum flexibility for the changing technological standards. It was considered comparable to the regulatory models of

[1386] Ibid 1.
[1387] Ibid.
[1388] The Office of the Australian Information Commissioner in the past has relied on 'mediated outcomes, rather than litigation' and education to inform businesses and government of their privacy obligations. Since the *Privacy Law (Amendment) Act 2014* (Cth) the increased powers given to the Commissioner have enabled a more 'resolute approach'. There have been more determinations since 2014 than during the previous 25 years: See Normann Witzleb, '"Personal Information" under the Privacy Act 1988 (Cth) – Privacy Commissioner v Telstra Corporation Ltd [2017] FCAFC 4' (2017) 45 *Australian Business Law Review* 188-192, 188. For general information and list of determinations see the website <http://www.oaic.gov.au>.
[1389] Dianne Nicol et al, 'Time to Get Serious About Privacy Policies: The Special Case of Genetic Privacy' (2014) 42 *Federal Law Review* 149.
[1390] Ibid 179.

Canada, New Zealand and the UK.[1391] Reidenberg recognised that there had emerged a global convergence or 'core set of standards for fair information practices' in democracies on First Principles, however considerable divergence in approach and interpretation of such laws.[1392] This was a divergence he saw as based on 'the core norms of a democratic society's organization regarding choices about the role of the state, market, and citizen in society' and leading to frequent confrontation. These differences reflecting the country's choice of governance depending on the 'role of the state, market and individual in the country's democratic structure'.[1393] He presented a theory of 'coregulations' through multinational coordination and cooperation based on active national regulatory agencies for data protection which he envisaged as the basis for 'deeper consensus on the integration of First Principles'.[1394]

Thirteen new Australian Privacy Principles (AAPs) commenced on 12 March 2014, replacing the National Privacy Principles and Information Privacy Principles.[1395] They regulate the handling of personal information by government agencies and some private organisations, promoting openness and transparency in the management of personal information. They have been viewed as addressing a variety of new threats to online information privacy caused by developments in technology and strengthening online privacy, limiting 'the ability of APP entities to data mine, amass information from online databases and cross match such unsolicited information with solicited information to obtain valuable data as to individual identity'.[1396] They have been seen as a movement towards the European approach to privacy while retaining a 'flexible principles-based approach'.[1397] While these principles have extended protection for privacy and will be updated in response to relevant court or tribunal decisions or changes in privacy legislation, they do not provide omnibus laws as found in the EU but apply to specific agencies and extend privacy protection in a limited manner.[1398] They are

[1391] The *Explanatory Memorandum* to the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012*.

[1392] Joel R Reidenberg, 'Resolving Conflicting International Data Privacy Rules in Cyberspace' (2000) 52 *Stanford Law Review* 1315, 1370.

[1393] Ibid 1319.

[1394] Ibid 1362.

[1395] The 13 APPs are to be found in Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Ch) which amended the *Privacy Act 1988* (Cth).

[1396] Niloufer Selvaduria, 'Protecting online information privacy in a converged digital environment – the merits of the new Australian privacy principles' (2013) 23 *Information & Communications Technology Law* 299, 309.

[1397] Ibid.

[1398] The Australian Privacy Principles provide for the open and transparent management of personal information, which includes a clearly expressed and current APP privacy policy; requires the entities covered by the principles, to give people the option of using a pseudonym or not identifying themselves; outlines when personal information which is solicited can be collected with a higher standard applying to the collection of "sensitive

indicative of a search for a practical solution without a firm basis on a philosophical or ethical foundation.

The main weakness of the APPs are the exceptions, the absence of a definition of privacy and the absence of a minimum standard for privacy. Only entities must comply with the principles, an organisation can use or disclose personal information for direct marketing if the individual has consented, or if the organisation is a contracted service provider, although an individual may request not to receive direct marketing. There are also quite extensive exceptions to the provision of access for organisations.

Further major changes to Australia's privacy law were recommended by the ALRC Report in September 2014,[1399] in particular the report recommended protection for serious invasions of privacy, providing 'certainly, consistency and coherence to the law'.[1400] In determining whether there is a cause of action competing interests need to be considered. These include, freedom of speech, freedom of the media, public health and safely and national security. One of the aims of the recommendations were to ensure that access to justice would be facilitated for people affected by serious invasions of privacy in the provisions of 'a range of means to prevent, reduce or redress serious invasions of privacy'.[1401] The report acknowledged significant 'uncertainties' in the existing law which would be addressed by these changes.[1402]

Despite many recent changes in the legal protection of privacy in Australia, privacy law is far from comprehensive and is somewhat disconnected from the rapid technological

information"; how unsolicited personal information should be dealt with is outlined; notification provision outline when and in what circumstances individuals should be notified about such factors as why the information is being collected; outlines the circumstances when the APP entity may use or disclose of personal information; provides when personal information can be disclosed for direct marketing; provides for the steps to be taken in protecting personal information before it is disclosed overseas; provides for circumstances when the adoption, use or disclosure of government related identifiers; provides for reasonable steps to be taken to ensure accurate, up-to-date and complete personal information; provides for the reasonable steps to be taken to protect the security of personal information; outlines the obligations in relation to access to the personal information held; and outlines the obligations in relation to the correction of personal information <http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/> .

[1399] ALRC Report 123, June 2014 Final Report 'Serious Invasions of Privacy in the Digital Era', released 3 September 2014.

[1400] Ibid 18.

[1401] Ibid 38.

[1402] Ibid 123, June 2014 Final Report 'Serious Invasions of Privacy in the Digital Era', released 3 September 2014: the matters that would be addressed by the changes include: supplementation of the common law; the recovery of damages for emotional distress; removing the uncertainty relating to the recovery of compensation would provide effective protection after wrongful disclosure;

developments in the global arena. I will examine the nature of privacy laws in the UK which has to some extent more recently been shaped by EU regulations.

6.3.3 Privacy regulation in the United Kingdom

There has been heavy reliance on the equitable cause of action for breach of confidence in the United Kingdom to resolve issues of privacy, although have not established a general cause of action for invasion of privacy.[1403] This was demonstrated in *Prince Albert v Strange.*[1404] Privacy was recognised as an essential part of the right to decide when and how property in etchings could be disclosed. The Lord Chancellor found that copies had been obtained either dishonestly or improperly with 'either a breach of confidence, or a positive crime committed, to obtain them'.[1405]

While the doctrine has shown 'adaptability to ill-sorted and disparate situations',[1406] one of the problems in relying on breach of confidence has been that traditionally it was important to establish that the information 'must have the necessary quality of confidence about it … [it] must have been imparted in circumstance importing an obligation of confidence' and 'there must be an unauthorized use of that information to the detriment of the party communicating it'.[1407]

An analysis of decisions by the 1990s indicated that the doctrine was no longer confined by 'relatively narrow boundaries'.[1408] Only one of the three elements was regarded as essential, 'it must be shown that a reasonable person who acquired the information would have realized that it was confidential'.[1409] It appeared therefore that the only way to accommodate privacy

[1403] *Wainwright and Anor v Home Office* [2003] 4 All ER 969, Lord Hoffman, 976 [19]; see also Sir Robert Megarry V-C in *Malone v Metropolitan Police Commissioner* [1979] Ch 344.

[1404] *Prince Albert v Strange* (1849) 47 ER 1302. In this case Mr Strange, a publisher who had obtained copies of Prince Albert's private etchings was found to have had actual or constructive knowledge of the confidential relationship between Prince Albert and the printer. The proposed publication of a catalogue describing the etchings was viewed by the Court as 'an intrusion – an unbecoming and unseemly intrusion' if not a 'sordid spying into the privacy of domestic life – into the home (a word hitherto sacred among us) … '[1404]. It was held in the England and Wales High Court (Chancery Division) that 'where privacy is the right invaded, postponing the injunction would be equivalent to denying it altogether"[1404]. Further that the "exclusive right and interest of the Plaintiff in the composition or work in question' had been established and he was entitled to an injunction to prevent publication. The possession of the etchings by the Defendant was held to have 'its foundation in a breach of trust, confidence, or contract'.

[1405] *Prince Albert v Strange* (1849) 47 ER 1302, 1308.

[1406] Helen Fenwich and Gavin Phillipson, 'Confidence and Privacy: A Re-Examination' (1996) 55(3) *Cambridge Law Journal* 447.

[1407] *Coco v A.N. Clarke (Engineers) Limited* [1969] R.P.C. 41, 47.

[1408] Fenwich and Phillipson, above n 1398.

[1409] Ibid 452.

intrusion within the breach of confidence doctrine was to provide greater flexibility in its application, in essence because 'privacy … is not relationship-based in the same way as confidence'.[1410] In *Douglas v Hello!* [1411] Keen LJ commented that, 'whether the resulting liability is described as being for breach of confidence or for breach of a right to privacy may be little more than deciding what label is to be attached to the cause of action'.[1412]

Despite the arguments over whether the issue is simply one of terminology, the rejection of a separate tort of privacy was confirmed by the UK Court of Appeal in *Wainwright v Home Office*.[1413] Lord Mummery considered to create a 'blockbuster' tort covering a wide variety of situations would create more problems that it solved. Lord Mummery preferred:

> incremental evolution, both at common law and by statute … of traditional nominate torts pragmatically crafted as to conditions of liability, specific defences and appropriate remedies, and tailored to suit significantly different privacy interests and infringement situations.[1414]

This incremental extension of existing torts was considered inadequate by authors such as, Markesinis and O'Cinneide who together with Fedtke and Hunter-Henin[1415] who proposed instead a consideration of foreign law, particularly French and German privacy laws, to enable a more coherent approach to privacy in the UK.[1416] They concluded that the incremental development of the law of confidence was 'inadequate, flawed, and dishonest,[1417] unsuited to the changing world following the introduction of the *Human Rights Act 1998* (UK) and the requirements of requirements of Article 8 of the European Convention on Human Rights. They found no evidence that political speech would suffer from enhanced privacy protection. In comparing the decision in *Von Hannover v Germany (Von Hannover)*[1418] and *Campbell v MGN Ltd*[1419] these authors preferred the decision of the Strasbourg court in *Von Hannover* which

[1410] Jonathan Morgan, 'Privacy, Confidence and Horizontal Effect: "Hello" Trouble' (2003) 62(2) *Cambridge Law Journal* 444, 451.
[1411] *Douglas v Hello!* [2001] Q.B. 967.
[1412] *Douglas v Hello!* [2001] Q.B. 967, 1012.
[1413] *Wainwright v Home Office* [2002] 3 WLR 405. In this case the plaintiffs obtained a remedy for strip-searches by claiming a tort of trespass to the person. This finding was rejected by the Court of Appeal and House of Lords where an extension of a breach of confidence was considered more appropriate to protect privacy.
[1414] *Wainwright v Home Office* [2002] 3WLR 405, 419. This decision was confirmed in the House of Lords, *Wainwright v Home Office* [2003] 4 All ER 969.
[1415] Basil Markesinis et al, 'Concerns and Ideas About the Developing English Law of Privacy (And How Knowledge of Foreign Law Might Be of Help) (2004) 52 *The American Journal of Comparative Law* 133.
[1416] Ibid 134.
[1417] Ibid 203.
[1418] *Von Hannover v Germany (Von Hannover)* [2004] ECHR 294.
[1419] *Campbell v MGN Ltd* [2004] UKHL 22.

'emphasized the crucial importance of privacy to individual well-being, and emphatically acknowledged the very real extent to which press intrusion can violate this essential value'.[1420]

In *Kaye v Robertson*[1421] the High Court granted an injunction to prevent publication of an article and photographs of the plaintiff, a well-known English actor with severe head injuries, taken in hospital. This interlocutory injunction was granted on the basis of a cause of action in malicious falsehood. Lord Justice Bingham considered in that case, in relying on malicious falsehood, it demonstrated 'yet again, the failure of both the common law of England and statute to protect in an effective way the personal privacy of individual citizens'.[1422] Lord Bingham referred to a statement by Professor Markesinis which criticized the development of English law which could often leave a plaintiff without a remedy if the facts of the case did not fit within the 'pigeon-hole of an existing tort'.[1423]

The recent developments in the UK have been influenced by the European Convention on Human Rights.[1424] The *Human Rights Act 1998* (UK) incorporates this Convention to some extent. However, the common law does not recognize the tort of invasion of privacy but the cause of action for breach of confidence has been extended to apply to certain breaches of privacy. In each case it must be demonstrated that there was a reasonable expectation of privacy in relation to the information. The public interest in the distribution of this information will then be considered and the two aspects of the claim balanced. Consent in most cases has been considered a defence. In examining the relationship between open justice and privacy in Australia and the UK, Rodrick[1425] found that in the UK privacy issues gained more prominence due to the impact of the *Human Rights Act 1998*.

The balancing of rights was illustrated by the decision in *Campbell v MGN Limited.*[1426] In this case the Court of Appeal overturned the decision of Morland J who had found in favour of

[1420] Basil Markesinis et al, 'Concerns and Ideas About the Developing English Law of Privacy (And How Knowledge of Foreign Law Might Be of Help) (2004) 52 *The American Journal of Comparative Law* 208.
[1421] *Kaye v Robertson* (1990) FSR 62.
[1422] *Kaye v Robertson* (1990) FSR 62, 70.
[1423] *Kaye v Robertson* (1990) FSR 62, 70.
[1424] *Campbell v MGN Ltd* [2004] UKHL 22 where Lord Nicholls acknowledged at [16] 'The European Convention on Human Rights, and the Strasbourg jurisprudence, have undoubtedly had a significant influence in this area of the common law for some years'.
[1425] Sharon Roderick, 'Open justice, privacy and suppressing identity in legal proceedings: "what's in a name?" and would anonymity "smell as sweet"?' *Emerging Challenges in Privacy Law: Comparative Perspective* Normann Witzleb, David Lindsay, Moira Paterson and Sharon Rodrick (eds) (2014) Cambridge University Press.
[1426] *Campbell v MGN Ltd* [2004] 2 AC 457.

Ms Campbell[1427] due to a breach of confidence involving the publication of additional information relating to her treatment for narcotic addiction and the surreptitious photographs taken. This decision was reversed by the House of Lords (by a majority of three to two) which established that '[t]he essence of the tort is better encapsulated now as misuse of private information.'[1428] In restoring the orders of the trial judge, the Court balanced the degree of privacy the claimant was entitled to under the law of confidence and the public interest in the release of information about the details of her drug therapy.

It introduced a 'respect' for privacy and by the introduction of the 'misuse of personal information' protects a person's 'private and family life, home and correspondence'. While this law affirms 'the existence of an independent right', Wacks, found this concept of 'private life' 'unhappily as vague as the "right to be let alone"'[1429] and 'invites obscurity and abstraction'.[1430]

The influence of European Union law on the development of privacy protection in the UK was demonstrated more recently in the High Court of Justice.[1431] A declaration was sought in the Divisional Court that section 1 of the *Data Retention and Investigatory Powers Act 2014* (UK) was inconsistent with European Union law. It was held that this Act was inconsistent in so far as:

> a) It does not lay down **clear and precise rules providing for access to and use of communications data retained pursuant to a retention notice** to be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating to such offences; and
>
> b) **Access to the data is not made dependent on a prior review by a court** or an independent administrative body whose decision limits access to and use of the data to what is strictly necessary for the purpose of attaining the objective pursued.[1432] (emphasis added)

[1427] Naomi Campbell, a celebrated fashion model, featured in an article on 1 February 2001 by the "Mirror" newspaper headed "Naomi: I am a drug addict". The article referred to her attempts at rehabilitation in a supportive manner, however the photographs showed Ms Campbell in the street

[1428] *Campbell v MGN Ltd* [2004] UKHL 22 at [14].

[1429] Raymond Wacks, *Privacy and Media Freedom* (Oxford University Press, 2013) 4.

[1430] Ibid 5.

[1431] *Davis & Ors v Secretary of State for the Home Department & Ors (Davis)* [2015] EWHC 2092 (Admin). Three separately issued claims were heard together: Case No: CO/3665/2014, CO/3667/2014, CO/3794/2014. The challenge to the validity of s 1 of the *Data Retention and Investigatory Powers Act 2017* (DRIPA) was made submitting that is was contrary to EU law. The DRIPA was legislation fast-tracked as emergency legislation following decision of the Court of Justice of the European Union (CJEU) in *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and* Ors [2015) QB 127 which concerned the CJEU's interpretation of Articles 7 and 8 of the Charter of Fundamental Rights of the EU.

[1432] *Davis & Ors v Secretary of State for the Home Department & Ors (Davis)* [2015] EWHC [114].

The EU therefore requires clear rules for access and use of data as well as for review. The claim involved the Court of Justice of the European Union's interpretations of Articles 7 and 8 of the Charter of Fundamental Rights of the EU, concerning the 'right to respect' for privacy and personal data. The decision in *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Re Landesregierrung (Digital Rights Ireland)* [1433] was found to be central to the High Court case and the reason the *Data Retention and Investigatory Powers Act 2014* (UK) had been introduced. The Court of Appeal in *Davis* concluded that the issue was of general and wide-reaching importance and referred two questions to the CJEU.[1434]

Although the introduction of the *Human Rights Act 1998* has established principles similar to EU law, despite the absence of a foundation for privacy on human dignity, the future impact of EU law on law in the UK is uncertain following the referendum decision of 23 June 2016for the UK to leave the EU.

6.3.4 The impact of self-regulation and markets in the United States

A tort of privacy has been recognized in the US, although the self-regulatory, market-dominated industries have opposed government attempts at providing effective legislation to protect privacy.

By 1960 Prosser[1435] was able to assess the development of this new tort in a detailed analysis of many of the privacy cases since the seminal 1890 article of Warren and Brandeis.[1436] While he considered there was a great deal of dispute until the 1930s about whether the right of privacy existed, by the 1960s he reported that it was recognised as existing by an 'overwhelming majority of American courts'.[1437] Prosser did not attempt a precise definition of the tort but considered that it consisted for four torts: intrusion upon seclusion or solitude or into private affairs; publicity which places a person in a false light; public disclosure of embarrassing private facts; and appropriation of someone's name or likeness. He attributed the reported

[1433] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources, Re Landesregierung (Digital Rights Ireland)* [2014] All ER (EC) 775. Case C-293/12) and Case C-594/12 were joined.
[1434] R *(on the application of Davis MP) v Secretary of State for the Home Department(Open Rights Group and ors intervening)* [2017] 1 All ER 62, 63. These questions were: the first, whether the CJEU in *Digital Rights Ireland* intended to lay down mandatory requirements of EU law and, second, whether the EJEU intended to expand the effect of Articles 7 and 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms 1950.
[1435] William L Prosser, 'Privacy' (1960) 48 *California Law Review* 383-423.
[1436] Ibid. Also see Warren and Brandeis, above n 640.
[1437] Ibid 386.

state of confusion in the law of privacy to a failure to distinguish these four forms of privacy intrusion.[1438] Prosser demonstrated some concern about the developments in the law of privacy and the limitations if any that should be considered to protect freedom of speech, although he acknowledged that real abuses and genuine public demand for privacy needed to be addressed.

Thierer[1439] has traced the legislative and regulatory efforts and enforcement challenges in the development of privacy law in the US, particularly in relation to online privacy which he recognized as 'one of the most contentious information policy debates of recent times'.[1440] Thierer advocated the adoption of alternative approaches to privacy protection because of the 'greater significance on both free speech rights and the importance of online commerce and innovation' relative to Europe. He did not consider the law would 'likely play as great a role due both to normative and practical constraints'.[1441] As an alternative he referred to the '3-E' solutions using education, empowerment and 'selective *enforcement* of existing targeted laws and other legal standards (torts, anti-fraud laws, contract law and so on)'.[1442] Thierer concluded that '[g]overnments should only intervene when clear harm can be demonstrated and user empowerment truly proves ineffective'.[1443]

In writing from an American perspective, Strahilevitz, recognized that privacy regulation in the US arises 'reactively' if at all, facing political difficulties '*because* the economics of privacy are difficult'. The harmonisation in information privacy in 'the transatlantic divide' was seen as 'one of the most profound challenges that legal regulators and judges must confront in the twenty-first century'.[1444] He suggests that for privacy harmonisation to succeed, a reinvigorated privacy tort protection or an agency that can deal with privacy issues in 'a proactive, nonsectoral way'.[1445]

[1438] Ibid 407.
[1439] Adam Thierer, 'The Pursuit of Privacy in a World Where Information Control Is Failing' (2013) 36 *Harvard Journal of Law & Public Policy* 409.
[1440] Ibid 410. Thierer referred to articles by Dennis D Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-regulation?* (2011) 34 *Seattle University Law Review* 439, 440 and Omer Tene, 'Privacy: The new generations' (2011) 1 *International Data Privacy Law* 15.
[1441] Thierer, above n 1417, 412.
[1442] Ibid 412.
[1443] Ibid 455.
[1444] Lior Jacob Strahilevitz, 'Towards A Positive Theory of Privacy Law' (2013) 126 *Harvard Law Review* 2010, 2012.
[1445] Ibid 2041.

The more recent developments in technology have led to a movement in regulatory policy towards collaborative governance. This could be seen in the 2012 White Paper.[1446] This proposed legislation uses fair information principles (FIPs) to assist the development of codes of conduct and multistakeholder processes. It is the multistakeholder[1447] organisations, such as the World Wide Web Consortium[1448] and the Internet Society[1449] that have established the standards and internet norms. The governance model of these multistakeholder organisations have been challenged by countries such as India and Russia that would prefer to see internet governance under the leadership of the United Nations.[1450] The multistakeholder organisations have been 'integral to the culture of the Internet' and a model of governance that has worked effectively in the past.[1451]

The existing regulatory framework has failed to address the emergence of threats to privacy that 'do not fit the standard analytical mould of the controller model'.[1452] It is no longer governments or organisations but individuals disclosing personal data on social networks that present a major problem for privacy. Individuals are often exempt from regulations.[1453] The US regulatory culture is not based on cooperation but rather adversarial regulatory style in contrast to the cooperative and consensus Dutch 'polder model of regulation' or consensus decision-making.[1454] The current proposed changes to privacy law in the US are seen by

[1446] The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (2012), this together with a Green Paper published in 2010 represented the US government position on privacy.

[1447] Joe Waz and Phil Weiser, 'Internet Governance: The Role of Multistakeholder Organizations" (2012) 10 *Journal on Telecommunications and High Technology Law* 331, 347. Describe these organisations as having representation from a diversity of economic and social interests and a representational role for civil society, 336.

[1448] On 23 June 2015, together with the Joint Technical Committee JTC 1, Information Technology of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), the World Wide Web Consortium announced approval of the MathML Version 3.0 2nd Edition as an ISO/IEC International Standard (ISO/IEC 40314:2015). MathML 3.0 is the mark-up language used in software and development tools for statistical, engineering, scientific, computational and academic expressions of math on the Web. MathML 3.0 improves accessibility authoring capabilities and can now be used both on its own, as before, or embedded in HTML <http://www.w3.org> .

[1449] The Internet Society was formed in 1991 with the goal of influencing the policy, governance, technology and development of the internet. <http://internetsociety.org>.

[1450] This is indicative of concern that the current internet governance should change. It is an issued discussed at the World Conference on International Telecommunications in Dubai, December 2012.

[1451] Joe Waz and Phil Weiser, 'Internet Governance: The Role of Multistakeholder Organizations' (2012) 10 *Journal on Telecommunications and High Technology Law* 331, 347.

[1452] Omer Tene, 'Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws' (2013) 74 *Ohio State Law Journal* 1217, 1219.

[1453] The EU framework provides exemptions for individuals under the "household exemption" ref Article 29 Data Protection Working Party, *Opinion 5/2009 on Online Social Networking*, 01189/09. WP 163. 12 June 2009, 5-7.

[1454] Dennis D Hirsch, 'Going Dutch? Collaborative Dutch Privacy Regulation and the Lessons It Holds for U.S. Privacy Law' (2013) *Michigan State Law Review* 83, 124. Hirsch attributes the history of cooperation to the necessity of consensus-building and negotiation to enable the system of dikes and pumps to reclaim land by local communities.

Hirsch as a hybrid form of regulation consisting of baseline regulations which is direct government regulation with some industry self-regulation, so that companies that follow an approved code of conduct would be deemed to comply with the statue and be entitled to a 'legal safe harbour'. Companies who failed to comply with the codes of conduct would be subject to government enforcement.[1455]

While the Federal Trade Commission in the US has endorsed privacy by design,[1456] the proposed changes support business and self-regulation above government regulation with limited 'baseline privacy principles' concerning the protection of consumer privacy by organisations.

6.3.5 Lessons from the European Union

Two distinct structural divergences have been identified in the US and in the EU respectively as 'liberal, market-based governance' and 'socially-protective, rights-based governance',[1457] otherwise referred to as a market-dominated policy as opposed to a rights-dominated approach. Reidenberg considered that the divergence draws on these distinct governance norms, consequently 'privacy conflicts will only be resolved by finding compatibility points or by convergence of those very governance norms'.[1458]

Allars examined the European model for privacy law and compared this with other relevant international models, particularly the Australian model, acknowledging the impact of OECD Guidelines[1459] and APEC Privacy Framework[1460] on the evolution of Australian privacy law.[1461] This analysis was illustrated by the different responses to privacy in Australian and the EU,

[1455] Ibid 87.

[1456] Edith Ramirez, 'Privacy By Design and the New Privacy Framework', a paper presented at the *Privacy by Design Conference* Hong Kong, 13 June 2012. Ramirez is a Commissioner of the Federal Trade Commission (FTC). She described the three core principles of the final privacy report of the FTC as: privacy by design, simplified choice, and transparency, (online) <https://www.ftc.gov>.

[1457] Joel R Reidenberg, 'Resolving Conflicting International Data Privacy Rules in Cyberspace' (2000) 52 *Stanford Law Review,* 1315.

[1458] Ibid 1370.

[1459] Margaret Allars, 'Cross-Border Transfer of Personal Information: Evolving Privacy Regulation in Europe and Australia' in (2014) Stefan Aufenanger et al (eds) *Media Convergence: Perspectives on Privacy* Vol 9, 113: the Organisation for Economic Co-operation and Development issued *Guidelines on the Protection of Privacy and Transborder Flows of Personal data* in 1980 at the same time as Convention 108 was developed. The Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108) set out principles for privacy protection (used as a basis for the EU Directive 95/46/EC).

[1460] The basis of the framework on privacy by the Asia-Pacific Economic Cooperation was the OECD Guidelines. These were voluntary and aimed at the development of consistent privacy protection in APEC countries while at the same time facilitating commerce by preventing the erection of barriers to information flow.

[1461] Allars, above n 1451, 106.

comparing the *Lindqvist*[1462] decision, where it was found that Mrs Lindqvist did not transfer data to a third country in breach of Article 25 of the EU Directive, to a decision of the federal Privacy Commissioner of Australia,[1463] which found breaches of two National Privacy Principles because any internet browser could access the financial information posted on the website. Allars commented that behind the factual similarity of these cases is a 'complex web of differences', however she also concluded that some claimed differences are based upon misconceptions and that others are dissolving as the EU and Australia reform their privacy laws.

In Europe, privacy as a 'personality' right has been significant and has influenced not only the development of EU law but also it has had a remarkable impact on the protection of personal data internationally. This has been in part due to EU demands for the security of information in cross-border movement of personal data. The EU has had a major influence on international information privacy,[1464] particularly since the 1995 Data Protection Directive[1465] and this has shaped the way businesses operate internationally.[1466] This influence has been referred to as the 'Brussels Effect'.[1467] In the twenty years prior to the passing of the Directive, the world's first comprehensive information privacy law was passed by the Hessian Parliament in Wiesbaden, Germany[1468] in 1970, then by other German states, the federal German government and other European nations all passed data protection statutes.

[1462] C101/01 Lindqvist [2003] ECR1-12971. Margaret Allars, 'Cross-Border Transfer of Personal Information: Evolving Privacy Regulation in Europe and Australia' in (2014) Stefan Aufenanger et al (eds) *Media Convergence: Perspectives on Privacy* Vol 9, 106-107.

[1463] *Own Motion Investigation v Bankruptcy Trustee Firm* [2007] PrivCmrA 5. In this matter the Privacy Commissioner investigated a bankruptcy trustee firm which has published personal information on its website. The Commissioner recommended that the bankruptcy files should be secured by password protection and certain information relating to whether bankrupts had breached the Bankruptcy Act should be removed from the file available to creditors.

[1464] Graham Greenleaf, 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108 (2012) 2 *International Data Privacy Law* 68, 77. He considered that the EU privacy model as 'the norm in most parts of the world with data privacy laws'.

[1465] This refers to Directive 95/46/EC of the European Parliament and of the Council (24 October, 1995) on the protection of personal data and the free movement of such data. This was passed before the development of social networks, cloud computing and Big data collection. Its effectiveness was limited by inconsistent application by member states.

[1466] David Scheer, 'For Your Eyes Only – Europe's New High-Tech Role: Playing Privacy Cop to the World (2003) *Wall Street Journal*, A1.

[1467] The phenomenon of the underestimated aspect of European power, which is contrary to popular perception of a weak and ineffective EU, has been described by Anu Bradford as the 'Brussels Effect'. It refers to the rules and regulations originating from Brussels which have had an international influence is areas such as food, chemicals, competition and the protection of privacy.: Anu Bradford, 'The Brussels Effect' (2012) 107 *North West University Law Review* 1.

[1468] Paul M Schwartz, 'The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures' (2013) 126 *Harvard Law Review* 1966, 1969.

On 25 January 2012[1469] the European Commission proposed a comprehensive modernisation of the 1995 data protection rules to ensure online privacy would be protected and assistance provided to Europe's digital economy. Apart from a revised framework for data protection, a 'right to be forgotten' was proposed to assist people in managing their data risks online, enabling them to delete personal data if there is not legitimate reasons for its retention. The personal data could relate to any information 'whether it relates to his or her private, professional or public life' and can be 'a name, a photo, an email address, bank details', 'posts on social networking websites', 'medical information' or even a computer IP address. According to Viviane Reding, the EU Justice Commissioner:

> The protection of personal data is a fundamental right for all Europeans, but citizens do not always feel in full control of their personal data. My proposals will help build trust in online services because people will be better informed about their rights …while making life easier and less costly for businesses. A strong, clear and uniform legal framework at EU level will help to unleash the potential of the Digital Single Market and foster economic growth, innovation and job creation. [1470]

A significant ruling[1471] on the right to be forgotten was made by the Court of Justice in 2014. The decision in the Court of Justice of the European Union, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (Case C-1131/12) [1472] (*Google Spain*) concerned personal data relating to debt recovery proceedings which had been reported in a daily newspaper in Catalonia. The matter had been transferred from a Spanish court to determine whether the 1995 Data Protection Directive 95/46 applied to a search engine such as Google, in particular to Google Spain, although the Google server was in the US and whether the right to be forgotten applied to provide protection for personal data. The Court ruled that EU rules apply to search engine operators, such as Google, even if the server is in the US; the right to be forgotten applied and an individual can apply to have the infringing personal information removed if it is inaccurate, inadequate, irrelevant or excessive.

[1469] European Commission, 'EDPS welcomes a "huge step forward for data protection in Europe", but regrets inadequate rules for the police and justice area' (Press Release, EDPS/12/2, 25 January 2012) <http://europa.eu/rapid/search.htm>.

[1470] Ibid.

[1471] *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (Case C-131/12) (13 May 2014) (*Google Spain*) – in 2010 a Spanish citizen, Mr Costeja González, filed a complaint with the national Data protection Agency, against Google Spain and Google Inc, as well as against a Spanish newspaper, La Vanguardia, for the publication of an auction notice containing details of his repossessed home on Google's search results. It was claimed that the issue has been resolved years before and the reference was irrelevant. It was found [28] that "in exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine 'collects' such data …[the activities] must be classified as 'processing' within the meaning of …" Article 2(b) of Directive 95/46. This processing of personal data carried out in the operation of the search engine could not "escape the obligations and guarantees" of the Directive [58].

[1472] *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (Case C-1131/12) *(Google Spain)* 13 May 2014.

It was held that the disclosure could not be justified by the economic interest of the search engine nor by any public interest in access to this information.[1473] However, the right to be forgotten is not an absolute right but must be balanced against rights such as freedom of expression and, depending of the circumstance of each case, and could be justified by 'the preponderant interest of the general public'[1474] in having access to such information if such a person played a role in public life.

It was found in this case that the processing of personal data by the search engine:

> carried out by the operator of a search engine is liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual's name, since that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet – information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty – thereby to establish a more or less detailed profile of him. Furthermore, the effect of the interference with those rights of the data subject is heightened on account of the important role played by the internet and search engines in modern society, which render information contained is such a list of results ubiquitous.[1475]

The problem arose, in this matter, when an internet user entered Mr Costeja González's name in the Google search engine. The results showed links to two pages of a daily newspaper with a large circulation.[1476] These pages contained announcements which mentioned Mr Gonazález in relation to a real estate auction connected to proceedings for the recovery of social security debts. These proceedings had been resolved for a number of years and therefore the reference to them 'was now entirely irrelevant'.[1477] Mr Gonazález lodged a complaint with the Spanish data protection agency which recognised his complaint against Google but not against the newspaper.

[1473] *Google Spain* C-131/12 (13 May 2014) at [81].
[1474] *Google Spain* C-131/12 (13 May 2014) at [100].
[1475] *Google Spain* C-131/12 (13 May 2014) at [80].
[1476] La Vanguardia Ediciones SL publishes a daily newspaper in Catalonia, Spain, *La Vanguardia* [14].
[1477] *Google Spain* C-131/12 (13 May 2014) [15].

Google Spain and Google Inc appealed to the Spanish High Court which referred three main questions[1478] to Court of Justice of the European Union for a preliminary ruling. It was held[1479] that 'the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to Article 2(b). Second, in applying Article 4(1)(a) of Directive 95/46 that 'the processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State'; third, 'the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages'; and fourth, 'in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public on account of its inclusion is such a list of results'. These rights override the economic interest of the operator and the interest of the general public in having access to this information but not if interference with his fundamental rights is justified due to his role in public life, access to the information relating to that person would not be removed.

The debate following this decision has been focussed on what many have referred to as 'a mistaken legal interpretation of the Directive that gave too much power to private entities to control public information access'.[1480] However it was considered that this criticism missed the point because the judgment is a 'reasonable reflection of the text of the Directive and the values embodied in it'.[1481] What should be the focus of the debate is 'the fundamental values at stake'[1482] and 'how – in a new regulatory regime'[1483] these fundamental values can be managed, particularly how a new regulatory regime can be tailored 'to the nuances of modern privacy protection'.[1484] It was considered that the decision which empowered 'an individual to control the use of his personal data was derived from the prioritization of individual privacy

[1478] The first, whether a search engine operator such as Google fell within the territorial scope of the Directive; the second, whether Google's activities amounted to 'processing of data'; and third, whether the Directive provided a right for individuals to require operators such as Google to erase data about themselves'.
[1479] *Google Spain* C-131/12 (13 May 2014) [100].
[1480] Harvard Law Review, 'Recent cases: Internet Law – Protection of Personal Data – Court of Justice of the European Union Creates Presumption That Google Must Remove Links to Personal Data Upon Request – Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos* (May 13, 2014)' (2014) 128 *Harvard Law Review* 735-742, 735.
[1481] Ibid.
[1482] Ibid 742.
[1483] Ibid 735.
[1484] Ibid 739.

rights in the Directive[1485] itself'.[1486] Other authors have considered that the decision has created significant risks for the protection of other fundamental rights, such as the freedom of speech. Furthermore, Frantiziou considered that without further legislation or court decisions, 'the companies on which an obligation to delete data has been imposed will in fact dictate the standard of when a right to be forgotten exists'.[1487]

Ratai examined the implications of Lessig's arguments concerning EU internet policies.[1488] While distinguishing those 'based on the concept of the information society and not on the concept of cyberspace as is Lessig's theory',[1489] Ratai found both concepts to be based on the 'social impacts of the use of technology'.[1490] He referred to the regulatory goals of the European Commission[1491] which concluded that 'the development of an information society has to be backed by a clear and stable regulatory framework'.[1492] Ratai identified four areas of potential regulation; telecommunications, intellectual property and privacy, media concentrations and the free movement of television broadcasting, however the serious technical limits to law enforcement and the importance of protecting human rights were seen as important.[1493] Ratai recognised a duality in the EU approach to regulation by realising that there must be regulation to balance freedom and control, however the EU was limited in its inability to influence the development of technology. He believed a possible answer could be in increased global cooperation to 'ensure that collective values will be able to regulate the emerging technical world'.[1494]

[1485] This refers to Directive 95/46 of the European Council passed in 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. It was proposed in 1990 in an era when the internet was different to its current form and passed before Google was founded. It also predates the European Union Charter of Fundamental Rights, particularly Articles 7 and 8 which imposes obligations on internet operators.

[1486] Harvard Law Review, above n 1458, 741.

[1487] Eleni Frantziou, 'Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12. *Google Spain, SL, Google Inc v Agencia Española de Protección de Datos*' (2014) 14 *Human Rights Law Review* 761, 770.

[1488] Balazs Ratai, 'Understanding Lessig: Implications for European Union Cyberspace Policy', *International Review of Law, Computers & Technology*, (2005) 19:3, 277-286.

[1489] Ibid, 278

[1490] Ibid 279.

[1491] The report entitled, 'Europe and the Global Information Society – Recommendations to the European Council' was prepared under the direction of Martin Bangemann, previous Vice-President of the European Commission, and accepted by the European Council at Corfu, 24-25 June 1994 <http://www.cyber-rights.org/documents/bangemann.htm> .

[1492] Ratai, above n 1480, 279.

[1493] Ibid.

[1494] Ibid 283.

Alternative proposals has been considered for adjudication of disputes including; an automatic delisting process, a public mediation model, a 'clear channel of appeal to a public authority', an arbitration board jointly funded by search engines and technical tools to allow for 'automatic expiry of posted content' or extensions to the robots.txt standard[1495] which could 'specify how search engines can notify webmasters of removals'.[1496] There was acknowledgement that some of the suggestions 'would appear to require legislative change in order to be put into effect' and that the task was complex. The debate about the most suitable regulatory model revealed fundamental unresolved issues. Concerns were reflected in such statements as, 'I'm not quite sure if that's the best person [the Data Protection Authority] to actually assess and resolve the conflict between the right to privacy and the freedom of expression'[1497]; 'it's important that the ruling however imperfect, is interpreted and applied on a consistent basis … '[1498] as well as a somewhat revealing comment by Ulf Buermeyer, Judge and Constitutional Law Expert:

> If Google is really implementing some kind of court, then I think it should really take up the challenge and implement some procedural rules that courts have come to adopt over the centuries. And the most important rule in this respect would in my view be that Google should implement some kind of fair trial in balancing interests.[1499]

These comments were made at in Advisory Council to Google report on the right to be forgotten, in the context of suggestions for legislative change to ensure the usual procedural fairness rules of civil and criminal procedure would be adopted.

Shortly after the decision in *Google Spain* was handed down, Google provided an online form for users to identify search results with links that disclose information 'irrelevant, outdated or otherwise objectionable' and started removing links a month later without disclosing the criteria or internal processes.[1500] Google established The Advisory Council to Google on the

[1495] This is a common facility the majority of robot authors offer to protect the world wide web community from unwanted accesses by their robots (these are programs that traverse web pages retrieving linked pages) <http://www.robotstxt.org> Robots are excluded from a server by the creation of a file which specifies an access policy for robots.

[1496] Report of The Advisory Council to Google on the Right to be Forgotten, 6 February 2015, 34-37.

[1497] Dorota Glawacka, Lawyer Helsinki Foundation for Human Rights, Advisory Council Meeting Warsaw, 30 September 2014.

[1498] Emma Carr, Director Big Brother Watch, Advisory Council Meeting London, 16 October 2014.

[1499] Ulf Buermeyer, Judge and Constitutional Law Expert, Advisory Council Meeting Berlin, 14 October 2014, referred to in 'The Advisory Council to Google on the Right to be Forgotten' <www.cil.cnrs.fr/CIL/IMG/pdf/droit_oubli_google.pdf> 34.

[1500] Julia Powles and Enrique Chaparro, 'How Google determined our right to be forgotten' (online) 18 February 2015, *theguardian* <http://www.the guardian.com/technology>. Powles and Chaparro reported that Google has subsequently removed 218,427 links by 18 February 2015, 3.

Right to be Forgotten soon after the decision in *Google Spain*. As the Report of this Council[1501] indicated it is not a right to be forgotten that has been established but the requirement for Google to remove links. As Verhoeven[1502] stated, '[l]aw cannot dictate to us to forget something. But we feel that a more correct approach is that you would redefine it as a right not to be mentioned anymore … '[1503] or as a right to make data more difficult to find. The Report referred to 'the process of removing links in search results based on queries for an individual's name as 'delisting'.[1504] When this process is completed the accessibility of the data to the general public is limited. Although the data is 'still available at the source site', there will not be a link from the search queries.[1505] If Google does not remove the link, the individual can challenge this decision 'before the competent Data Protection Authority or Court'.[1506] The 'asymmetries of power' were referred to by Powles and Chaparro[1507] when they concluded that 'if we concede that the internet is public space, that the web is the public records, then Google, on its logic, is the custodian and indexer of our personal records' and the 'right to delist:[1508]

> forces us to look at the privatised reality of digital life, and take responsibility for what we see. Internet companies have been successful in making us believe that the internet is 'public space', when in reality, it is just an algebraic representation of privately owned services'.

Powles and Chapparo considered that Google in not waiting for guidance from the regulators, it has promoted its own role in regulating the digital environment and they admonished regulators 'to take a more active and central role in these kind of legal and ethical debates'.[1509]

From the US perspective the 'right to be forgotten' was viewed by Rosen as 'the biggest threat to free speech on the Internet in the coming decade'.[1510] Rosen considered that this new right addressed the problem people face in forgetting their past when photos, bogs and tweet live forever, however it highlighted the 'diametrically opposed approaches to the problem of privacy and publication in Europe and the US'. The example given concerned a person with a

[1501] Report of The Advisory Council to Google on the Right to be Forgotten, (6 February 2015) <https://www.google.com/advisorycouncil/>.
[1502] Editor in Chief De Standaard, Advisory Council Meeting Brussels, 4 November 2014.
[1503] Powles and Chaparro, above n 1492, 3.
[1504] Ibid 4.
[1505] Ibid 4.
[1506] Ibid 4.
[1507] Ibid 1-7.
[1508] Ibid 5.
[1509] Ibid 3.
[1510] Jeffrey Rosen, 'The Right to Be Forgotten' (2012) 64 *Stanford Law Review Online* 88 – 92, 88 <http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten>.

criminal conviction who in France could access the 'right of oblivion' whereas in the US the publication of a criminal history is protected by the First Amendment. Rosen criticised the European tradition of 'declaring abstract privacy rights in theory' which they fail to enforce. Because the right to be forgotten could be asserted against the publisher of content as well as search engines Rosen considers it will have a chilling effect on freedom of speech and ensure that the internet will not remain 'as free and open as it is now'.[1511] However, the Attorney General of California more recently has recommended 'surprise minimization' as a privacy protection measure, particularly for the 'mobile ecosystem' to ensure that consumers are not surprised by unauthorised or unexpected data collection.[1512] This reflects a desire by some for an adjustment in US policy and a recognition of the global environment of privacy regulation.

Conflicting policies and differing regulatory systems internationally have been highlighted by interactive applications operating in a 'virtually borderless'[1513] environment. The similarities and differences between the protection of privacy in the EU and the US, particularly in relation to online privacy which have been related to factors such as 'privacy perceptions, differences in cultural values and legislative restrictions'. Baumer et al found that the legal protection for online privacy was much stricter in the EU and contrasted the definitions of personal information in these countries.[1514]

There appears to be move towards convergence of privacy regulations in the future, dictated in part by the need for cross-border information flow requiring a degree of legal interoperability, and pressure from European regulations 'consciously designed to promote international convergence' and a 'higher level of protection of personal information', despite the 'two different core sets of values'[1515] in the 'transatlantic clash'.[1516] International

[1511] Ibid 2.

[1512] Kamala D Harris, 'Privacy On The Go: Recommendations for the Mobile Ecosystem; (January 2013) Report by the Attorney General, California Department of Justice <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/privacy_on_the_go.pdf>.

[1513] David L Baumer, Julia B Earp and J C Poindexter, 'Internet privacy law: a comparison between the United States and the European Union' (2004) *Computers & Security* 400.

[1514] Ibid ref: 2.1 and 2.2 Section 8(8) of the 2003 version of OPPA describes personal information as "first and last name; home and other physical address; e-mail address; social security number; telephone number; and any other identifier that the Commission [FTC] determines identifies an individual; or information that is maintained with, or can be searched or retrieved by means of, data described immediately above; Article 2(a) of the 1995 Information Direction defines *personal data* as 'any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, psychological, mental, cultural or social identity…"

[1515] James Q Whitman, 'The Two Western Cultures of Privacy: Dignity Versus Liberty' (2004) 113 *Yale Law Journal* 1151, 1219.

cooperation and coregulation have been considered as possibilities in a global digital world where the international flow of personal data challenges privacy protection.

Reding highlighted the importance of 'shared values such as the rule of law, democracy, freedom, solidarity, economic development and stability' in the development of the internet.[1517] She considered that international legal standards would form a framework for the protection of privacy and data while facilitating the free flow of information across boundaries. With the announcement in the US of plans for a Consumer Privacy Bill of Rights,[1518] Reding was optimistic that there could be a synergy between European and US privacy legislation.[1519]

The common law and civil law view of privacy are contrasted to expose 'ill-defined values' that Eltis considers no longer serve 'the intended rationale'.[1520] The North American and Canadian view was described as based on a view of what one can reasonable expect and the idea of seclusion. This is contrasted with the European view of privacy as a 'personality right', based on the dignity of the person not property.[1521] It is this view of privacy which as seen as an ally of access, more easily reconciled to openness in the courts and the responsibility to protect the privacy of parties.[1522] Eltis recommends a comparative analysis at a time when people are speaking to each other using the same word with different meanings so that what results is a 'technological "tower of Babel" with frustrating hurdles'.[1523] This is found when comparing the different meaning of privacy between the EU and the US. Eltis considered that a conceptual certainty for privacy is be found in the European tradition.[1524] She considered that privacy and access have been viewed by policy makers as 'adversarial terms' in an era of 'conceptual uncertainty'.[1525] This conflict could be resolved by the courts by viewing

[1516] Ibid 1153.
[1517] Ibid 85.
[1518] On 23 February 2012 the Obama Administration announced a 'Consumer Privacy Bill of Rights' to protect privacy so that users would have the right to control personal information about themselves, how it is collected and used; a right to easily understand and access information about privacy and security practices; a right to expect companies would collect, use and disclose personal data in a manner consistent with the way the information was provided; a right to the secure and responsible handling of personal data; a right to access and correct personal data; a right to reasonable limits on the personal data collected and retained by companies and the right to insure companies will adhere to the Consumer Privacy Bill of Rights. <www.whitehouse.gov>
[1519] *Aspen Report*, above n 1481, 83.
[1520] Eltis, above n 413, 311.
[1521] Ibid 314.
[1522] Ibid 315.
[1523] Eltis, above n 813, 75.
[1524] Ibid.
[1525] Ibid.

privacy as deriving from human dignity allowing judges to 'be more inclined to use their discretion to protect litigants' (and other participants') privacy if doing so would not be regarded as sacrificing openness or transparency'.[1526]

While McCrudden found that the use of human dignity, 'has not given rise to a detailed universal interpretation' nor a 'substantive meaning'[1527], it can provide 'a language in which judges can appear to justify how they deal with issues such as the weight of rights, the domestication and contextualization of rights, and the generation of new or more extensive rights'.[1528] Floridi, however, considered that privacy protection 'should be based directly on the protection of human dignity'[1529] which he interprets as 'the outcome of a specific philosophical anthropology that sees humanity as essentially different from any other species … in a way that deserves special consideration'.[1530] It is human dignity that Floridi viewed as the fundamental concept for the interpretation of informational privacy in the GDPR and generally in the EU.

The lessons from the EU developments in privacy law are that access with privacy is possible by providing protection for the 'essence' of privacy based on an inalienable personality right embodied in data protection, rather than on a right to the property in the information itself. The EU has enacted protection for personal data, while recognising the inalienable aspects of privacy. The EU regulations have recognised, in the 'right to be forgotten', the right to data protection which 'connects with notions such as informational self-determination and control' rather than ideas of 'identity and autonomy'[1531] and so facilitating the adoption of more specific and consistent regulation.

6.4 Conclusion

My research question—to what extent *should* the innovative technologies of Web 2.0 be used to enhance access to justice in the digital era—was formulated to analyse the potential of innovative technologies to enhance access to justice and to address the need for a reassessment of what this concept means online. The more complex regulatory environment with overexposure of personal data in the digital era has demanded regulatory change,

[1526] Eltis, above n 413 316.
[1527] Christopher McCrudden, 'Human Dignity and Judicial Interpretation of Human Rights' (2008) 19 *The European Journal of International Law* 655-724, 724.
[1528] Ibid.
[1529] Floridi, above n 561, 308.
[1530] Ibid.
[1531] Hildebrandt, above n 1294, 190.

particularly for the courts using the innovative technologies of Web 2.0. While their use by the courts to date has been cautious, reflecting the regulatory prudence advocated by Brownsword, such innovative technologies have demonstrated the future possibilities to fulfil legal needs and enhance the administration of justice. These applications have the potential to transform access and create a digital pathway to justice which is efficient, cost effective and can provide increased transparency.

In this thesis I have applied the interpretation of Web 2.0 as a concept encompassing a smart system, constantly changing as new technologies are invented, distinguishing the more static Web 1.0 from Web 2.0 and subsequent technological developments. It is possible to analyse the development of the World Wide Web as a series of major changes like versions of software such as Web 1.0, 2.0, 3.0 and possibly 4.0 and beyond. Tim Berners-Lee,[1532] the inventor of the World Wide Web and director of the World Wide Consortium, W3C, has discussed the continuing dynamic nature of the technological changes. Although Berners-Lee referred to the semantic web and the web of data and has been critical of 'Web 2.0' as a term, the interpretation of authors such as O' Reilly (discussed in detail in Chapter One) and Berners-Lee are not in conflict to the extent that they recognise the dynamic nature of the Web that has become 'the world'. Aghaei, Nematbakhsh and Farsani[1533] have traced the development of the World Wide web from Web 1.0 to Web 4.0, referring to Web 1.0 as the 'web of cognition', Web 2.0 as the 'web of communication, Web 3.0 as the 'web of co-operation' and Web 4.0 as the 'web of integration', however they do not provide clear demarcations between the web 'versions' or exact definitions. The critical issue for access to justice is whether a 'symbiotic' web or an 'intelligent' web using artificial intelligence will provide greater access. Analysing such an issue would provide a challenging problem for future research.

In the first chapter I provided the background to digital access to justice by discussing the innovative developments of Web 2.0 and the disruptive regulatory environment in which they have developed. I described the theoretical and empirical methodology to be used to examine the issues identified to frame the limits of access to justice. An issue discussed in Chapter One was the possible use of an index to measure digital access to justice. Just as the search

[1532] Tim Berners-Lee and Mark Fischetti, *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by its inventor* (1999, HarperCollins).
[1533] Sareh Aghaei, Mohammad Ali Nematbakhsh and Hadi Khosravi Farsani, 'Evolution of the World Wide Web: From Web 1.0 to Web 4.0' (2012) 3 *International Journal of Web & Semantic Technology* 1.

for a perfect index to measure access to justice is illusive, similarly, measurement of digital access to justice is challenging. As demonstrated in earlier chapters, it is possible to measure specific quantifiable aspects of online access, such as the number of matters heard in eCourtroom, or the volume of communicated Tweets on Twitter. It is also possible to measure indicators such as the financial savings for parties if they do not have to attend a physical courtroom. The measurement of intangible costs such as the disclosure of personal information or the affront to human dignity by the invasion of privacy remains difficult to assess, the multiple dimensions of such a complex can effectively analysed using qualitative analysis and innovative methodology.

In Chapter Two I examined access to justice in the digital era in the context of the literature relating to access to justice, particularly the access to justice movement, finding that the transformation in the digital environment has impacted on the tension between access and privacy. The open access and transparency made possible by digital technologies have changed the nature of open courts. Not only has there been a transition from the practical obscurity of hard copy records to an era of infinite digital availability but a transformation for some hearings from the use of physical courtrooms to virtual courts. These changes have opened up the necessity of increased protection for personal data.

The increased tension between access and privacy, caused by overexposure, was the subject of the discussion in Chapter Three. This tension has impacted on the boundary between public and private information. An analysis of the literature on privacy revealed considerable divergence of views with authors such as Nissenbaum and Floridi reconceptualising privacy for the digital era and searching for a new equilibrium. Eltis has commented on the inoperability of 'first generation privacy laws' which adopted a more binary view and focused on the difference between personal and non-personal data or private and public information: [1534]

> The better view of privacy harm is one able to distinguish between otherwise trivial (oftentimes publicly available) information once labelled "personal" and the information that is central to identity in context. It is this view that empowers courts to differentiate between the two for purposes of protecting litigants before them.[1535]

[1534] Eltis, above n 413, 98.
[1535] Ibid.

Eltis supported a central role for identity in the formulation of effective privacy laws in the digital era. This focus can be found in a recent decision of the Full Court of the Federal Court of Australia, *Privacy Commissioner v Telstra Corporation Limited* in which the link between information and identity was analysed.[1536] Justices Kenny and Edelman clarified that in determining whether 'whether the individual's identity is apparent or can be ascertained' account must be taken of other information with which it can be combined.[1537]

A more detailed analysis of Web 2.0 applications, OSNs and the exposure of personal information, was presented in Chapter Four. This extended the discussion of openness in earlier chapters and the opportunities applications such as Twitter can provide for the courts, particularly by allowing direct communication with the public, improving transparency and confidence in the courts. The unique challenges of OSNs were analysed to determine the regulatory controls necessary to prevent the transformation from transparency to overexposure. The use of Twitter by the Supreme Court of Victoria demonstrated that such OSNs can be used to improve access to justice applying the regulatory prudence and legitimacy advocated by Brownsword, however, the loss of privacy is exacerbated in the online digital era where OSNs, such as Facebook and Twitter, provide a new dimension in social interaction and communication. They have created challenges for the courts by offering direct communication but an anarchical space where legal regulations have become negotiable. Users of online services have been severely compromised by the misuse of personal data and its accompanying aggregation, sale and deliberate or inadvertent disclosure.

Empirical research, using the mixed methodology of case studies and questionnaire, were used in Chapter Five to analyse the use of eCourtroom, a virtual court, in the Federal Circuit Court and Federal Court of Australia. These methods were chosen to enhance the finding of the theoretical assessment of the revolutionary changes in the digital environment and provide

[1536] *Privacy Commissioner v Telstra Corporation Limited* (2017) 262 IR 230. This appeal concerned the narrow question of statutory interpretation concerning whether the words, 'about an individual' had substantive operation. It was held that they did. The National Privacy Principle 6.1 and the definition of 'personal information' in s 6 of the *Privacy Act 1988* (Cth) were read together. It was held that while the definition of 'personal information' is very broad, it is constrained by the three requirements: first, it must be held by the organisation; secondly, it must be 'about' the individual; and thirdly, it must be 'about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion'. This judgment was concerned with the definition of 'personal information' as it applied before 12 March 2014 and did not clarify the definition as it currently stands. The definition, 20 October 2016 states: '***personal information*** means information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.' Interpretation of these changes will be evident in privacy cases in the future.

[1537] Normann Witzleb, "'Personal Information" under the Privacy Act 1988 (Cth) – Privacy Commissioner v Telstra Corporation Ltd [2017] FCAFC 4' (2017) 45 *Australian Business Law Review* 188-192, 190.

details for a discussion in this concluding chapter of the strategies required to enhance access to justice. The case studies analysed the transcript of proceedings available to the public to determine the efficiencies of procedures, the regulatory controls and privacy issues. The questionnaire sought open-ended responses to general questions about the experience of Registrars of the Federal Court of Australia and Federal Circuit Court using eCourtroom. Questions were directed to the perceived advantages and disadvantages of using such a virtual court and as well as the access and privacy issues that may arise. The final question was directed at the future use of eCourtroom using additional innovative technologies. It was found that the use of a virtual court was efficient for the matters listed and achieved the system objectives by the use of a modular design which was flexible, tested and evaluated to retain the most effective elements, while open to further augmentation, such as the use of skype-like facilities to extend its use. [1538] The use of eCourtroom also facilitated public access to transcripts in compliance with the principle of open courts and demonstrated the development of ex ante court-controlled rules to provide public access and protect personal information, particularly information that is personally identifying and sensitive, yet must be disclosed in the context of litigation.

In this chapter I have addressed various strategies for resolving the tension between access and privacy to ensure that innovative technologies are able to enhance access to justice. These have been discussed in the context of the current regulatory framework and the necessity for change. An analysis of privacy legislation in Australia, the UK, US and EU was presented to highlight the necessity for a change in the digital era from an understanding of privacy as property in the information itself to the protection of personal information based on the essence of privacy as an inalienable right linked to identity.

As the decision in *Google Spain* has shown, in the digital era, it will not be possible for the courts to control all sensitive information collected and made available for the internet's infinite memory. The regulatory response in the EU has clarified the need for an ex post model of regulation to enhance the effectiveness of privacy regulation and provided guidelines

[1538] In 2013 an online survey was conducted by the Court regarding eServices. The objective was to gauge the future use and user satisfaction with eLodgment, use of the Commonwealth Portal and eCourtroom and obtain a user profile. The targeted group were the top three eLodgers and counter/fax filers from each Court Registry. The Deputy District Registrars and Directors of Court Services assisted in identifying the suitable firms and in obtaining consent for the survey.

for the implementation of the *Google Spain* decision.[1539] Since Google established an official request process on 29 May 2014 they have evaluated over two million URLs and assessed over one million requests for removal.[1540] It is the national Data Protection Authorities that analyse how a search result should be deleted and assess extraterritorial application such as whether the search result should be delisted when searches are made from other countries. The jurisdictional reach of the national Data Protection Authorities remains a matter for a case by case analysis in the Court of Justice of the European Union.

The regulations in the EU and the Court of Justice of the European Union have established a clear legal framework for managing the impact of online personal data release to ensure that there is a place for the rule of law in the corporate review processes of companies like Google and Facebook.

6.5 Recommendations

This thesis makes two main recommendations:

(1) The first that a *more extensive use of the innovative technologies of Web 2.0* should be made by Australian courts to enhance access to justice.

(2) The second that a focus on *ex post protection*, such as the 'right to be forgotten' or right to delist should be considered to rectify inadvertent or deliberate disclosure of personal data and resolve the tension between access and privacy by re-instating a measure of practical obscurity for the protection of identity.

[1539] European Union, Article 29 Data Protection Working Party, *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on 'Google Spain and Inc v Agencia Española De Protección de Datos (AEPD) and Mario Costeja González' C-131/12).* These guidelines provided a list of criteria, referred to as 'a flexible working tool' to assist the Data Protection Authorities in their decision-making in accordance with the relevant national legislation. The aim of the guidelines was to achieve a fair balance between fundamental rights and interest. No information is to be deleted from the original source with the practical impact of de-listing on freedom of expression and access to information limited. The data subjects' entitlement to request de-listing is recognized, especially where there is a clear link between the data subject and the EU. The ruling recognized that the processing carried out by the operator of a search engine is liable to significantly affect the fundamental rights to privacy and the protection of personal data.

[1540] Google, *Transparency Report European privacy request for search removals* <https:www.google.com/transparencyreport/removals/europeprovacy/?ht=en-GB>.

(1) *More extensive use of Web 2.0 applications*

The empirical research in chapters four and five have demonstrated, while the use of Web 2.0 applications by courts is at an early stage, their use has improved communications between the courts and the public, provided efficiencies to enhance access to justice in a way not possible in the analogue era. The implementation of Web 2.0 has been seen in the use of online applications by courts such as the Supreme Court of Victoria, as well as by the Federal Court of Australia and the Federal Circuit Court. These courts have implemented applications using modular stages which allow testing and evaluation[1541] before proceeding with the next stage, exercising the regulatory prudence recommended by Brownsword.

The use of OSNs, such as those used by the Supreme Court of Victoria, has achieved direct communication with the legal profession and the public for procedures, judgments and information about the appointment and retirement of judges without the necessity for the intervention of the media as the medium of communication. This court has used Web 2.0 as a platform for the provision of services with controlled collaboration. Despite the limited use by courts, it has been recognized that OSNs cannot be ignored. The challenges they present were discussed by at a symposium in 2016 for members of the judiciary, administrators and researchers.[1542]

The use of eCourtroom, analysed in the previous chapter, has been directed to specific matters and has provided an efficient court for the resolution of procedural issues, such as substituted service in bankruptcy matters which has saved time and costs for parties and the courts. The procedures have been regulated by the Courts to protect the security and privacy of personal data and provide the opportunity for direct communication with the public, transparency through the availability of a public transcript and to improve confidence in the courts. Similar transformations from physical to virtual courts can be

[1541] See above n 1514, discussion of 2013 survey of users of eServices.

[1542] Australasian Institute of Judicial Administration and the Judicial Conference of Australia, *A Symposium: Challenges of Social Media for Courts & Tribunals*, 26-27 May 2016, Melbourne. An Issues Paper was presented by Marilyn Krawitz, 'Challenges of Social Media for Courts & Tribunals'. This referred to the profound impact that social media has had on Australian courts in a short period. It examined the nature of social media; situations when judicial officers and tribunal members or their families use OSNs personally; the benefits and the risks and situations when it has been used maliciously to denigrate to denigrate or threaten the judiciary and tribunal members. Discussions focused on what could be done to develop strategies and policies to manage OSNs. It was generally acknowledged that personal use should be passive, however, controlled use by the courts could provide a useful channel of communication.

found in courts such as those in the UK[1543] and Canada[1544], where online justice is being implemented making 'the internet, rather than courthouses, the place where citizens access justice'.[1545]

The specific technologies analysed, eCourtroom and Twitter, have been shown to have the capacity to address barriers to access to justice such as costs, communication, delay, inefficiencies and geographical distance. There has been considerable research on the more traditional barriers to access such as the costs of litigation, court delays, as well as access to justice in developing countries and access for disadvantaged groups. There has been limited research on barriers such as privacy and the exposure of personal information. While most Web 2.0 applications can improve communications and access to information, overcoming a number of traditional barriers, paradoxically they also have the capacity to create new barriers such as the exposure of personal data. Brownsword and Goodwin identified human rights, such as privacy, as boundary markers which determine limitations on new technologies.[1546]

This thesis recommends the more extensive use of Web 2.0 applications with the reservation that the provision of privacy protection needs to be addressed.

[1543] Lord Justice Briggs has recommended that an online court to resolve claims up to £25,000 should be established to improve access to justice: See Judiciary of England and Wales, *Civil Courts Structure Review: Final Report* (*Biggs Report)* (2016) <https://www.judiciary.gov.uk>. For an assessment on the proposed online courts see: Special Issue, (2017) 36 *Civil Justice Quarterly*: Andrew Higgins and Adreian Zuckerman (eds) 'Lord Justice Brigg's "SWOT" Analysis Underlines English Law's Troubled Relationship with Proportionate Costs'; Masood Ahmed, 'A Critical View of Stage 1 of the Online Court' ; Judge Nigel Bird, 'Open Justice in an Online Post Reform World: A Constant and Most Watchful Respect'; Victoria McCloud, 'The Online Court: Suing in Cyberspace'; Stuart Sime, 'Appeals after the Civil Courts Structure Review'; 'Rabeea Assy, 'Briggs' Online Court and the Need for a Paradigm Shift'; John Sorabji, 'The Online Solutions Court-A Multi-door Courthouse for the 21st Century'; Pablo Cortés, 'The online Court: Filling the Gaps of the Civil Justice System'; Inbar Levy, 'Taking Enforcement Seriously'.

[1544] Victoria McCloud, 'The Online Court: Suing in Cyberspace: How the Online Court challenges us to raise our legal and technological game so as to ensure access to justice' (2017) 36 *Civil Justice Quarterly* 34-50. In assessing the proposed Stage 1 Online Court in the UK, McCloud uses the examples of MyLawBC and the Civil Resolution Tribunal in Canada. Stage 1 of the Online Court, essentially a lawyer-free court, is analysed and the challenges in implementing the automated system by which litigants are assisted to identify their case. She concluded that the compulsory automated procedure is 'substantially unique, and uniquely ambitious', although it has the potential to achieve cost savings and improve access to justice. Stage 2 is to consist of a mix of conciliation and case management, conducted by case managers and Stage 3 will be a determination by judges on the documents, by telephone, by video or a face-to-face hearing but no traditional trial will be provided: cf Masood Ahmed, 'Introduction' (2017) 36 *Civil Justice Quarterly* 12-22,15.

[1545] Darin Thompson, 'The Online Justice Experience in British Columbia' (online) 22 November 2016, *Society for Computers & Law*. The Civil Resolution Tribunal (CRT) in British Columbia on 13 July 2016 began operating an online civil tribunal with strong similarities to proposed online courts <http://www.scl.org>.

[1546] Brownsword and Goodwin, above n 64, Chapter 8. In this chapter Brownsword and Goodwin identify six boundary markers: human dignity, harm, equality, nature, property and privacy, concluding that privacy is threatened from all angles and as such the most discussed aspect of technological change.

Similarly new technologies that have been developed to provide artificial intelligence and robotics operate by the collection and linking of data and can also expose personal information and threaten privacy. A detailed examination of the impact of these technologies on law is beyond the framework of this thesis however they offer considerable material for future research.[1547]

(2) *Ex post protection.*

A more extensive use of Web 2.0 applications would be facilitated by a change a focus from incremental ex ante legal protection of privacy to the adoption of ex post protection for personal information. Inadvertent and deliberate disclosure of personal data online has intensified the tension between access and privacy. This can be resolved by the adoption of procedures to delete online links and restore a measure of protection for personal information by modifying the overexposure caused by aggregation, extensive distribution and permanency of online data. It would recognise the inevitability of the online release of personal information and the altered digital environment which has removed the practical obscurity of past physical records.

This change in focus can be seen in the development of the 'right to be forgotten' or 'de-link' concept in EU law, developed following the decision in *Google Spain*[1548] in an attempt to regulate the accessibility of legally published online information. This has not been proposed as a simple solution but seen as a complex balancing act in the clash between access to information and privacy.[1549] A problem of how much is reversible or archivable in the digital world and to what extent the past concept of 'practical obscurity' can be achieved is yet to be determined in the future, but it is not an issue that can be ignored due to the problem of overexposure of personal information.

[1547] Artificial intelligence provides assistance in areas such as automatic legal text classification and summarisation; automated information extraction from legal databases and texts; data mining for ediscovery and computational models of evidential reasoning: see the work of the International Association for Artificial Intelligence and Law <http://www.iaail.org>. The developments in robotics is also considered to be an emerging technology with legal and regulatory implications particularly in the area of healthcare and autonomous vehicles. Data collection is essential for their operation and therefore privacy and data protection an issue which may be a barrier to their use without adequate regulation: see Chris Holder et al, 'Robotics and law: Key legal and regulatory implications of the robotic age (Part 1 of 11) (2016) 32 *Compter Law & Security Review* 383-402.
[1548] See discussion of *Google Spain* at 254-257 of this thesis.
[1549] Luciano Florida, 'Right to be Forgotten: A Diary of the Google Advisory Council Tour' (2014) <http://www.philosophyofinformation.net/right-to-be-forgotten-a-diary-of-the-google-advisory-council-tour/>. This diary consists of a series of articles written by Floridi for *The Guardian* as a member of the Council.

The protection of personal information based on the EU concept of privacy as human dignity provides a substantive framework linking privacy, identity and human dignity and has the potential to resolve the tension between access to justice and privacy. In protecting personal data and privacy in the 'infosphere' this balance can be found in recognition of this link, clearly articulated by Floridi in his ontological interpretation of informational privacy, between personal information and personal identity. This is an acknowledgment that a person '*is* her or his information' and that personal information is 'a constitutive part of someone's personal identity and individuality',[1550] and as such that person is entitled to as a 'fundamental an inalienable right'[1551] to the protection of personal information and personal identity. It is a relational view of identity and privacy, supported by authors such as Hildebrandt and Altman, which allows individuals to realign themselves and reconfigure identity in the online world.[1552]

In conclusion, Web 2.0 is an 'achievable and implemented reality',[1553] where the internet is used as a platform for the delivery of services and for direct communication. Access to justice can be enhanced by the provision of a digital pathway providing more direct open communication for the courts, savings in time and costs and enhanced transparency. However, without recognition of the radical transformation in the informational environment, the need for a role for data ethics and a philosophy of information, there is a risk that the rule of law in the future will be replaced by the rule of technology. How courts respond to the challenges and opportunities offered by new technologies will determine whether access becomes a 'limitation on the attainment of the fundamental goal of justice. The ideal has to be the delivery of justice: not just access to a chance of it.'[1554]

The formulation of legitimate and effective regulations to achieve this has been challenged by the commercial value of personal data, by new technological means of surveillance and by confusion over what is public and what is private in online spaces. Information such as personal data has been recognised as a form of capital which requires the development of

[1550] Floridi, above n 547, 195.
[1551] Ibid.
[1552] Hildebrandt, above n 1280, 82; Irwin Altman, 'Privacy Regulation: Culturally Universal or Culturally Specific?' (1977) 33 *Journal of Social Issues* 66-84 and "Privacy: "A Conceptual Analysis"" (1976) 8 *Environment and Behaviour* 7-29.
[1553] Floridi, above n 547.
[1554] Roger Smith, 'After the Act: what future for legal aid?' (2012) 9(2) *Justice Journal* 8-23, 17. Paper presented at the Tom Sargant memorial annual lecture 2012, Freshfields Bruckhaus Deringer LLP, London, 16 October 2012.

public policies to facilitate data flow to develop the digital economy. The barrier to achieving free data flow has been viewed as the regulatory gap between 'inconsistent laws and policies in different countries, as well as legal uncertainty, preventing cloud computing from scaling up and driving down costs for consumers and businesses'.[1] However, the economic advantages of an open yet trusted internet provide interesting lessons for legal regulation. As Reding, the EU Justice Commissioner, explained:

> If we don't want to hinder technological development, we have to encourage trust in emerging technologies. Technology is designed to serve people. It must respect citizens' rights and freedoms. It must contribute to economic and social progress on both sides of the Atlantic, trade expansion and citizens' well-being.[1555]

The balance between the use of technology and protection of personal data needs to be found to ensure that technology remains a facilitator of access, particularly with the volume of user-generated content and unregulated disclosure. This has been seen by George and Scerri as challenging traditional legal regulation creating issues which are 'widespread', some 'evidently illegal, others border on legality, yet others are undesirable or morally indefensible'.[1556] Breaches of security and confidentiality in legal practice have also been raised as serious concerns with the use of interactive technologies, particularly the risks associated with the compromise of client information.[1557]

It is not possible for courts to ignore the technological innovations of the digital era in providing access to justice, however, in so doing there is a need to address the role for the rule of law because the 'accelerating transition from law to technological management'[1558] has begun. What will be of significance for the rule of law in the future is the way in which we engage with innovative technologies, particularly the most disruptive innovations, preserving normative values and providing effective protection for personal information in the online provision of access to justice.

[1555] Viviane Reding, 'Privacy standards in the digital economy: enhancing trust and legal certainty in transatlantic relations' (Speech, 11/210, Brussels, 23 March 2011), 2.
[1556] Carlisle George and Jackie Scerri, 'Web 2.0 and User-Generated Content: legal challenges in the new frontier' (2007) (2) *Journal of Information, Law and Technology* <http://go.warwick.ac.uk/jilt/2007_2/george_scerri>.
[1557] Coralie Kenny and Tahlia Gordon, 'Social media issues for legal practice' (2012) 66 *Law Society Journal* 66, 68.
[1558] Brownsword and Goodwin, above n 64, 50.

Brownsword has recognised that there will need to be a role for the rule of law and technological regulation in the future where the 'normative regulatory environments will co-exist and co-evolve with technologically managed environments'[1559]. He has warned that a regulatory environment needs to allow the normative values of law to flourish. Of significance is the need to recognise the role of data ethics in the future regulatory environment. As authors such as Hildebrant, [1560]Brownsword and Goodwin[1561] have suggested, in order to preserve the legal protection of the rule of law in the context of a democratic society, it will be necessary to take a stand for the substance of the norms and the values we wish to retain. Of concern is that ['l]aw is not, in essence, a body of technical rules, uncouth formulae … '[1562] nor can it be reduced to an algorithmic expression. At its 'very foundation it is 'conceived and derived from values', '*human* values' that 'lie at the heart of every individual and at the heart of society … ';[1563] human values based on human dignity and integrity.[1564]

The challenge for law in the use of innovative technologies of Web 2.0 is to find 'the appropriate balance between rules and values'[1565] and in striking this balance to enable innovative technologies to enhance access to justice. This will entail retaining the 'underdeterminancy' vital for constitutional democracy, as suggested by Hildebrandt, and allowing a deliberate disconnect from the online world to achieve the practical obscurity of the past.

[1559] Brownsword, above n 68, 14.
[1560] Hildebrandt, above n 1280, 219.
[1561] Brownsword and Goodwin, above n 64, 23.
[1562] W J V Windeyer, *Legal History* (2nd ed, revised), Law Book Company of Australasia, 1957), 3. Although, Windeyer was writing well before the digital era, he recognized the essential role of law in society and while it may 'lag behind the demands which social development makes' it makes it possible for people to live in communities.
[1563] Chief Justice James Allsop, 'Values in Law: How They Influence and Shape Rules and the Application of Law' Paper presented at the Centre for Comparative and Public Law, Faculty of Law, University of Hong Kong, Hochelaga Lecture Series 2016 (20 October 2016) 1.
[1564] Ibid 3.
[1565] Ibid 13.

BIBLIOGRAPHY

A *Articles*

Abel, Laura K, 'Evidence-Based Access to Justice' (2009) 13 *University of Pennsylvania Journal of Law and Social Change* 295

Abril, Patricia Sanchez, 'Recasting Privacy Torts in a Spaceless World' (2007) 21 *Harvard Journal of Law & Technology* 1

Acquisti, Alessandro, Leslie K Joh, and George Loewenstein, 'What is Privacy Worth?' (2013) 42 *The Journal of Legal Studies* 249

Adams, Leigh, 'Clarity brought to service in cyberspace: electronic transactions laws fill the gap' (2010) 10(10) *Insolvency Law Bulletin* 168

Aghaei, Sareh, Mohammad Ali Nematbakhsh and Hadi Khosravi Farsani, 'Evolution of the World Wide Web: From Web 1.0 to Web 4.0' (2012) 3 *International Journal of Web & Semantic Technology* 1

Allen, Anita L, 'Privacy-as Data Control: Conceptual, Practical, and Moral limits of the Paradigm' 1999-2000) 32 *Connecticut Law Review* 861

Altman, Irwin, 'Privacy: "A Conceptual Analysis"' (1976) 8(1) *Environment and Behavior* 7

Amery, Grant, 'Social Media and the Legal System: Analyzing Various Responses to Using Technology from the Jury Box' (2010-2011) 35 *The Journal of the Legal Profession* 112

Assy, Rabeea, 'Briggs' Online Court and the Need for a Paradigm Shift' (2017) 36 *Civil Justice Quarterly* 70

Bamberger, Kenneth A, 'Foreword: Technology's Transformation of the Regulatory Endeavor' (2011) 26 *Berkeley Technology Law Journal* 1315

Barbry, Eric, 'Web 2.0: Nothing Changes … but Everything is Different' (2007) 65 *Communications & Strategies* 91

Barnes, Susan B, 'A privacy paradox: Social networking in the United States' 9 *First Monday* 11 <http:/firstmonday.org>

Barrett, Jonathan, 'Open Justice or Open Season? Developments in Judicial Engagement with New Media' (2001) 11 *Queensland University of Technology Law and Justice Journal* 1

Barrett, Jonathan, and Luke Strongman, 'The Internet, the Law, and Privacy in New Zealand: Dignity with Liberty?' (2012) 6 *International Journal of Communication* 127

Baumers, David, L., and Julia B Earp, and J. C. Poindexter, 'Internet privacy law: a comparison between the United States and the European Union' (2004) *Computers & Security* 400

Bedner, Adriaan and Jacqueline A.C Vel, 'An Analytical framework for empirical research on Access to Justice' (2010) 1 *Law, Social Justice & Global Development Journal* 1

Bellis, Judith, 'Public access to court records in Australia: An international comparative perspective and some proposals for reform' (2010) 19 *Journal of Judicial Administration* 197

Bennett, Colin J, 'In Defence of Privacy: The concept and the regime' (2011) 8(4) *Surveillance & Society* 485

Bennett, Colin J., 'Privacy Advocacy from the Inside and the Outside: Implications for the Politics of Personal Data Protection in Networked Societies' (2011) 13(2) *Journal of Comparative Policy Analysis: Research and Practice* 125

Bennett Moses, Lyria, 'Adapting the Law to Technological Change: A Comparison of Common Law and Legislation' (2003) 26 *UNSW Law Journal* 394

Bennett Moses, Lyria, 'Understanding Legal Responses to Technological Change: The Example of *In Vitro* Fertilization' (2005) 6 *Minnesota Journal of Law, Science & Technology* 505

Bennett Moses, Lyria, 'Recurring Dilemmas: The Law's Race to Keep Up With Technological Change' (2007) 2007 *University of Illinois Journal of Law, Technology & Policy* 239

Bennett Moses, Lyria, 'Why have a Theory of Law and Technological Change?' (2007) 8 *Minnesota Journal of Law, Science & Technology* 589

Bennett Moses, Lyria, 'Creating Parallels in the Regulation of Content: Moving from Offline to Online' 33 *UNSW Law Journal* 581

Bennett Moses, Lyria, 'Agents of Change: How the Law "Copes" with Technological Change' (2011) 20 *Griffith Law Review* 763

Bennett Moses, Lyria, 'How to Think about Law, Regulation and Technology: Problems with "Technology" as a Regulatory Target"' (2013) 5(1) *Law, Innovation and Technology* 1

Bennett Moses, Lyria, and Janet Chan, 'Using Big Data for Legal and Law Enforcement Decisions, Testing the New Tools' (2014) 37 *UNSW Law Journal* 643

Bepko, Arminda Bradford, 'Public Availability or Practical Obscurity: The Debate over Public Access to Court Records on the Internet' (2005) 49 *New York School Law Review* 968

Bermant, Gordon, 'Courting the Virtual: Federal Courts in an Age of Complete interconnectedness' (1999) 25 *Ohio Northern University Law Review* 527

Bermant, Gordon and Winton D Woods, 'Real Questions about the Virtual Courthouse' (1994) 78 *Judicature* 64

Bernal, P.A., 'Web 2.5: The Symbiotic Web' (2010) 24(1) *International Review of Law, Computers & Technology* 25

Bernal, Paul A., 'A Right to Delete?' (2011) 2(2) *European Journal of Law and Technology* 1

Bingham, Lord, 'The Rule of Law' (2007) 66 *Cambridge Law Journal* 67

Birnhack, Michael, 'Reverse Engineering Informational Privacy Law' (2012) 14 *Yale Journal of Law & Technology* 24

Birnhack, Michael and Elken-Karen Niva, 'Does Law Matter Online? Empirical Evidence on Privacy Law Compliance' (2011) 17 *Michigan Telecommunication Technology Law Review* 337

Birnhack, Michael, Eran Toch and Irit Hadar, 'Privacy Mindset, Technological Mindset' (2014) 55 *Jurimetrics* 55

Black, Julia, 'Regulatory Conversations' (2002) 29 *Journal of Law and Society* 163

Black, Julia, 'Critical Reflections on Regulation' (2002) 27 *Australian Journal of Legal Philosophy* 1

Black, Michael E J, 'New Technology Developments in the Courts – Usages, Trends and Recent Developments in Australia' (2007) 31 *Melbourne University Law Review* 1017

Blackham, Alysia and George Williams, 'Australian Courts and Social Media' (2013) 38 *Alternative Law Journal* 170

Blackham, Alysia and George Williams, 'Courts and social media: Opportunities, challenges and impact' (2014) 17(9) *Internet Law Bulletin* 210

Blackham, Alysia and George Williams, 'Social Media and Court Communication (July 2015) *Public Law* 403

Bloom, Mark D, David M Olenczuk and Richard L Wynne, 'Reorganizing in a Fish Bowl: Public Access vs. Protecting Confidential Information' (1999) 73 *American Bankruptcy Law Journal* 775

Bloustein, Edward J., 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' (1964) 39 *New Your University Law Review* 962

Boehning H Christopher and Daniel J Toal, 'Authenticating Social Media Evidence' (2 October 2012) 248(65) *New York Law Journal, Technology Today* <http://www.newyorklawjournal.com>

Bosland, Jason and Ashleigh Bagnall, 'An Empirical Analysis of Suppression Orders in the Victorian Courts: 2008-12' (2013) 35 *Sydney Law Review* 671

boyd, danah m, and Nicole B.Ellison, 'Social Network Sites: Definition, History, and Scholarship' (2007) 13 *Journal of Computer-Mediated Communication* 210

boyd, danah, 'Privacy and Publicity in the Context of Big Data' (2010) <http://www.danah.org>

boyd, danah, and Alice E Marwick, 'Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies' (2011) *Social Science Research Network* <http://ssrn.com/abstract=1925128>

Bradford, Anu, 'The Brussels Effect' (2012) 107(1) *Northwestern University Law Review* 1

Brennan, Sir Gerard, 'Why be a Judge?' (1996) 14 *Australian Bar Review* 89

Brescia, Raymond H et al, 'Embracing Disruption: How Technological Change in the Delivery of Legal Services can Improve Access to Justice' (2015) 78 *Albany Law Review* 553

Browning, John G., 'Why Can't We Be Friends? Judges' Use of Social Media' (2014) 68 *University of Miami Law Review* 487

Brownsword, Roger, 'Code, Control, and Choice: Why East is East and West is West' (2005) 25 *Legal Studies* 1

Brownsword, Roger, 'Neither East Nor West, Is Mid-West Best?' (2006) 3(1) *SCRIPT-ed* 15 <https://ssrn.com/abstract=1127125>

Brownsword, Roger, 'Lost in Translation: Legality, Regulatory Margins, and Technological Management' (2011) 26 *Berkeley Technology Law Journal* 1322

Brownsword, Roger, 'The shaping of our on-line worlds: getting the regulatory environment right' (2012) 20 *International Journal of Law and Information Technology* 249

Brownsword, Roger, 'In the year 2061: from law to technological management (2015) 7 *Law, Innovation and Technology* 1

Buckley, Isaac Frawley, 'In defence of "take-down" orders: Analysing the alleged futility of the court-ordered removal of archived online prejudicial publicity' (2014) 23 *Journal of Judicial Administration* 203

Burd, Roxanne, and Jacqueline Horan, 'Protecting the right to a fair trial in the 21st century – has trial by jury been caught in the world wide web?' (2012) 36 *Criminal Law Journal* 103

Burdon, Mark, 'Privacy Invasive Geo-Mashups: Privacy 2.0 and the Limits of First Generation Information Privacy Laws' (2010) 1*Journal of Law, Technology & Policy* 1

Burdon, Mark, 'Contextualizing the Tensions and Weaknesses of Information Privacy Data Breach Notification Laws' (2011) 27 *Santa Clara Computer & High Technology Law Journal* 63

Burdon, Mark and Paul Telford, 'The Conceptual Basis of Personal Information in Australian Privacy Law' (2010) 17(1) *eLaw Journal: Murdoch University Electronic Journal of Law* 1

Burdon, Mark, and B Lane and P von Nessen, 'Data Breach Notification Law in the EU and Australia – Where to Now?' (2012) 28 *Computer Law and Security Review* 296

Burney, Brett, 'Meeting Your Clients on the Ramp' (2010) *Michigan Bar Journal* 60

Butler, Des, 'A Tort of Invasion of Privacy in Australia?' (2005) 29 *Melbourne University Law Review* 339

Buttar, Shahid, 'DHS Issues Process and Privacy Guidance on State and Local Drones' (6 January 2016) <http://eff.org>

Bygrave, Lee A, 'Strengthening privacy protection in the Internet environment: A modest program of action' (2006) 11 *Privacy Law and Policy Reporter* 222

Cabral, James E and Thomas M Clarke, 'Using Technology to Enhance Access to Justice' (2012) 26 *Harvard Journal of Law & Technology* 241

Caldwell, Jillian, 'Protecting Privacy Post *Lenah*: Should the Courts Establish a New Tort or Develop Breach of Confidence?' (2003) 26 *UNSW Law Journal* 90

Campbell, Roderick, 'Access to the Courts and Its Implications' (1999) 1 *UTS Law Review* 127

Cannon, Andrew, 'Policies to Control Electronic Access to Court Databases' (2001) 6 *Journal of Judicial Administration* 100

Cappelletti, Mauro, Bryant Garth and Nicolò Trocker, 'Access to Justice: Comparative General Report' III Zugang Zum Recht 40 *Journal of Comparative and International Private Law* 669

Cappelletti, Mauro, and Garth Bryant, Nicolò Trocker, 'Access to Justice: Comparative General Rep (1976) 40 *The Rabel Journal of Comparative and International Private Law* 669

Carlisle, George, and Jackie Scerri, 'Web 2.0 and User-Generated Content: legal challenges in the new frontier, (2007) 2 *Journal of Information, Law Technology* 1

Chavan, Abhijeet, 'Mobile Strategies for Legal Services – Using Technology to Enhance Access to Justice' 2012) 26 *Harvard Journal of Law & Technology 267*

Clarke, Roger, 'Introduction to Dataveillance and Information Privacy, and Definitions of Terms' (Original, 15 August 1997, revised 24 July 2016) <http://www.rogerclarke.com/DV/Intro.html>

Clarke, Roger, 'Beyond the OECD Guidelines: Privacy Protection for the 21st Century' (2000) <http://www.rogerclarke.com>

Clarke, Roger, 'Persona Missing, Feared Drowned: The Digital Persona Concept, Two Decades Later' (revised 2013) <http://www.rogerclarke.com>

Clarke, Roger, 'Privacy and Social Media: An Analytical Framework' (2014) 23 *Journal of Law, Information and Science* 169

Cockfield, Arthur, 'Towards a Law and Technology Theory' (2004) 30 *Manitoba Law Journal* 383

Cockfield, Arthur, 'Protecting the Social Value of Privacy in the Context of State Investigations Using New Technologies' (2007) 40(1) *University of British Columbia Law Review* 41

Cockfield, Arthur, and Jason Pridmore, 'A Synthetic Theory of Law and Technology' (2007) 8 *Minnesota Journal of Law, Science & Technology* 475

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

Colby, Jeremy A., 'You've Got Mail: The Modern Trend Towards Universal Electronic Service of Process' (2003) 51 *Buffalo Law Review* 337

Conklin, William E., 'Whither Justice? The Common Problematic of Five Models of "Access to Justice"' (2001) 19 *Windsor Yearbook of Access to Justice* 297

Conley, Amanda et al, 'Sustaining Privacy and Open Justice in the Transition to Online Court Records: A Multidisciplinary Inquiry' (2012) 71 *Maryland Law Review* 772

Cunliffe, Emma, 'Open Justice: Concepts and Judicial Approaches' (2012) 40 *Federal Law Review* 385

De Zwart, Melissa, Sal Humphreys and Beatrix van Dissel, 'Surveillance, Big Data and Democracy: Lessons for Australia From the US and UK' (2014) 37 *UNSW Law Journal* 713

DiBiana, Margaret, M, 'Ethical Risks Arising From Lawyers' Use Of (And refusal to use) Social Media' (2011) 12 *Delaware Law Review* 179

DiNucci, Darcy, 'Fragmented Future' (1999) 32 *Design & New Media* 220

Doty, Nick and Deirdre K. Mulligan, 'Internet Multistakeholder Processes and Techno-Policy Standards: Initial Reflections on Privacy at the World Wide Web Consortium' (2013) 11 *Journal on Telecommunications and High Technology Law* 135

Doyle, Justice John, 'The Courts and the Media: What Reforms are Needed and Why?' (1999) 1 *University of Technology Sydney Law Review* 25

De Rosnay, Melanie Dulong, 'Peer-to-peer as a design principle for law: Distribute the law' (2015) 6 *Journal of Peer Production* <http://peerproduction.net>

Eltis, Karen, 'Can the Reasonable Person Still be "Highly Offended"? An Invitation to Consider the Civil Law Tradition's Personality Rights-Based Approach to Tort Privacy' (2008) 5 *University of Ottawa Law & Technology Journal* 199

Eltis, Karen, 'The Judicial System in the Digital Age: Revisiting the Relationship Between Privacy and Accessibility in the Cyber Context' (2011) 56 *McGill Law Journal* 289

Eltis, Karen, 'Breaking Through the "Tower of Babel": A "Right to be Forgotten" and How Trans-Systemic Thinking Can Help re-Conceptualize Privacy Harm in the Age of Analytics' (2011) 22 *Fordhall Intellectual Property, Media & Entertainment Law Journal* 69

Epstein, Dmitry, Merrill C Roth and Eric P S Baumer, 'It's The Definition, Stupid! Framing of Online Privacy in the Internet Governance Forum Debates' (2014) 4 *Journal of Information Policy* 144

Erevelles, Sunil, Nobuyuki Fukawa and Linda Swayne, 'Big Data consumer analytics and the transformation of marketing' (2016) 69 *Journal of Business Research* 897

Fenwich, Helen, and Gavin Phillipson, 'Confidence and Privacy: A Re-Examination' (1996) 55 *Cambridge Law Journal* 447

Finegan, Jeanne C., and Craig E Johnson, 'New Media Creates New Expectations for Bankruptcy Notice Programs' (2011) *American Bankruptcy Institute Journal* 40

Fitzgerald, Anne et al, 'Open Access to Judgments: Creative Commons Licences and the Australian Courts' (2012) 19 *Murdoch University Law Review* 1

Fitzgerald, Brian, 'Software as Discourse: The Power of Intellectual Property in the Digital Architecture' (2010) 18 *Cardozo Arts & Entertainment Law Journal* 337

Fitzgerald, Brian, Cheryl Foong and Megan Tucker, 'Web 2, social networking and the courts' (2011) 35 *Australian Bar Review* 281

Fitzgerald, Brian, and Cheryl Foong, 'Suppression Orders after *Fairfax v Ibrahim*: Implications for Internet Communications (2013) 37 *Australian Bar Review* 1

Fleming, Michael F, and Christina L Kunz, 'Foreword: The Long Wave of Developing Law' (2011) *William Mitchell Law Review* 1666

Flint, David, 'Law shaping technology: Technology shaping the law' (2009) 23(1-2) *International Review of Law, Computers & Technology* 5

Floridi, Luciano, 'The ontological interpretation of informational privacy' (2005) 7(4) *Ethics and Information Technology* 185

Floridi, Luciano, 'Four challenges for a theory of informational privacy' (2006) 8 *Ethics and Information Technology* 109

Floridi, Luciano, 'The Construction of Personal Identities Online' (2011) 21 *Minds & Machines* 477

Floridi, Luciano, 'The Informational Nature of Personal Identity' (2011) 21 *Minds & Matters* 549

Floridi, Luciano, 'Turing's three philosophical lessons and the philosophy of information' (2012) 370 *Philosophical Transactions of the Royal Society* 3536

Floridi, Luciano, 'On Human Dignity as a Foundation for the Right to Privacy' (2016) 29(4) *Philosophy & Technology* 307 <http://link.springer.com/article/10.1007/s13347-016-0220-8>

Floridi, Luciano and Mariarosaria Taddeo, 'What is data ethics?' (2016) 374(20160360) *Philosophical Transactions of the Royal Society* 1

Frantziou, Eleni, 'Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12. *Google Spain, SL, Google Inc v Agencia Española de Protección de Datos*' (2014) 14 *Human Rights Law Review* 761

Fraru-Meigs, Divian, 'From Secrecy 1.0 to Privacy 2.0: Who Controls What, (2010) 123 *Revue Freancaise D'Etudes Americaines* 1<http://www.cairn.infor/revue-francaise-d-etudes-americaines-2010-1-page-79.htm>

Fried, Charles, 'Privacy' (1968) 77 *Yale Law Journal* 475

Friedman, David, D, 'Does Technology Require New Law? (2001) 25 *Harvard Journal of Law & Public Policy* 71

Friedman, Lawrence, 'Digital Communications Technology and New Possibilities for Private Ordering' (2003) 9 *Roger Williams University Law Review* 57

Friedman, Lawrence, 'Access to Justice: Some Historical Comments' (2009) 37 *Fordham Urban Law Journal* 2

Froomkin, A M, 'The Death of Privacy?' (2000) 52 *Stanford Law Review* 1461

Gallie, W B, 'Essentially Contested Concepts' (1956) 9 *the Aristotelian Society* 167

Golafshani, Nahid, 'Understanding Reliability and Validity in Qualitative Research' (2003) 8 *The Qualitative Report* 597

Gageler, Justice Stephen, 'What is information technology doing to the common law?' (2014) 39 *Australian Bar Review* 146

Galanter, Marc, 'Why the "haves" Come Out Ahead: Speculations on the Limits of Legal Change' 1974) 9 *Law and Society Review* 165

Ganguly, Maya, 'Private Pictures, Public Exposure: Papparazzi, Compromising Images, and Privacy Law on the Internet' (2009) 26 *Wisconsin International* 1140

Garth, Bryant G, 'Access to Justice: The Newest Wave in the Worldwide Movement to Make Rights Effective' (1978) 27 *Buffalo Law Review* 181

Gavison, Ruth, 'Privacy and the Limits of the Law' (1980) 89 *Yale Law Journal* 460

Gelman, Lauren, 'Privacy, Free Speech, and "Blurry-Edged" Social Networks' (2009) 50 *Boston College Law Review* 1315

George, Carlisle and Jackie Scerri, 'Web 2.0 and User-Generated Content: legal challenges in the new frontier' (2007) 2 *Journal of Information, Law & Technology* (now renamed *European Journal of Law and Technology*) 2 <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2007_2/george_scerri>

Gibson, Judith, 'Should judges use social media?' (2013) *American Bar Association Formal Opinion* 462

Gibson, Judith, 'Judges, cyberspace and social media' (2015) 12 *The Judicial Review* 237

Glancy, Dorothy J, 'The Invention of the Right to Privacy' (1979) 21 *Arizona Law Review* 1

Goodwin, Morag, Bert-Jaap Koops and Ronald Leenes (eds.) *Dimensions of Technology Regulation* (Wolf Legal Publishers, 2010)

Goel, Sharad et al, 'The Structural Virality of Online Diffusion' (2016) 62 *Management Science* 180

Gramatikov, Martin, 'A Framework for Measuring the Costs of Paths to Justice' (2009) 2 *The Journal Jurisprudence* 111

Gramatikov, Martin, and Maurits Barendrecht, Jin Ho Verdonschot, 'Measuring the Costs and Quality of Paths to Justice: Contours of a Methodology' (2011) 3 *Hague Journal on the Rule of Law* 349

Greacen, John, 'Introduction – Using Technology to Enhance Access to Justice' (2012) 26 *Harvard Journal of Law & Technology* 243

Greenleaf, Graham, 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convent 108' (2012) 2 *International Data Privacy Law* 68

Greenleaf, Graham, '"Modernising" data protection Convention 108: A safe Basis for a global privacy treaty?' 2013) 29 *Computer Law & Security Review* 43

Griffith, Heather L, 'Understanding and Authenticating Evidence From Social Networking Sites' (2012) 7 *Washington Journal of Law and Technology* 209

Griffith, Tom et al, 'Twitter, suppression and the court' (2012) 15(3) *Internet Law Bulletin* 42

Hall, Mark A, and Ronald F Wright, 'Systematic Content Analysis of Judicial Opinions' (2008) 96 *California Law Review* 63

Hartzog, Woodrow, and Frederic Stutzman, 'The Case for Online Obscurity' 2013) 101 *California Law Review* 1

Harvey, Christina Vassiliou, Mac R McCoy and Brook Sneath, '10 Tips for Avoiding Ethical Lapses When Using Social Media' (January 2014) *Business Law Today,* American Bar Association <https://www.americanbar.org/publications/blt/2014/01/03_harvey.html>

Heindl, Sabiene, 'Justice Cowdroy confirms costs order in iiNet case' *Internet Law Bulletin* (November/December 2010) 144 <http:www.lexisnexis.com.au>

Hetcher, Steven, 'Changing the Social Meaning of Privacy in Cyberspace' (2001) 15 *Harvard Journal of Law & Technology* 149

Hickford, Mark, Law Commission, New Zealand *A Conceptual Approach to Privacy* (2007)

Hildebrandt, Mireille, 'Legal and technological normativity: more (and less) than twin sisters' (2008) 12 *Techné Research in Philosophy and Technology* 3

Hildebrandt, Mireille and Laura Tielemans, 'Data protection by design and technology neutral law' (2013) 29 *Computer Law & Security Review* 509

Hildebrandt, Mireille and Bert-Jaap Koops, 'The Challenges of Ambient Law and Legal Protection in the Profiling Era' (2010) 73(3) *The Modern Law Review* 428

Himma, Kenneth Einar, 'Towards a Theory of Legitimate Access: Morally Legitimate Authority and the Right of Citizens to Access the Civil Justice System' (2004) 79 *Washington Law Review* 101

Hirsch, Dennis D, 'Going Dutch? Collaborative Dutch Privacy Regulation and the Lessons It Holds for U.S. Privacy Law' (2013) 1 *Michigan State Law Review* 83

Hirsch, Dennis D, 'The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulations?' (2011) 34 *Seattle University Law Review* 439

Hodge, Matthew J, 'The Fourth Amendment and Privacy Issues on the "new" Internet: Facebook.com and MySpace.com' (2006) 31 *Southern Illinois University Law Journal* 95

Holder, Chris et al, 'Robotics and law: Key legal and regulatory implications of the robotic age (Part 1 of 11) (2016) 32 *Computer Law & Security Review* 383

Hough, Bonnie Rose, 'Let's Not Make it Worse: Issues to Consider in Adopting New Technologies – Using Technology to Enhance Access to Justice' (2012) 26 *Harvard Journal of Law & Technology* 256

Hough, Bonnie Rose and Richard Zorza, 'Tech-Supported Triage: The Key to Maximizing Effectiveness and Access' 278-292 in James E Cabral et al, 'Using Technology to Enhance Access to Justice' (2012) 26 *Harvard Journal of Law & Technology* 241

Hsieh, Hsiu-Gang and Sarah E Shannon, 'Three Approaches to Qualitative Content Analysis' (2005) 19 *Qualitative Health Research* 1277

Hughes, Patricia and Janet E Mosher (eds) 'Forward' (2008) 45 *Osgoode Hall Law Journal*, xxix.

Hughes, Patricia, 'Law Commissions and Access to Justice: What Justice Should We Be Talking About?' (2008) 45 *Osgood Hall Law Journal* 773

Janoski-Haehlen, Emily, 'The Courts Are All a "Twitter": The Implications of Social Media Use in the Courts' (2011) 46 *Valparaiso University Law Review* 43

Johnson, R B and A J Onwuegbuzie, 'Mixed Methods Research: A Research Paradigm Whose Time Has Come' 33 *Educational Researcher* 14

Kahn, Jonathan, 'Privacy as a Legal Principle of Identity Maintenance' (2003) 33 *Seton Hall Law Review* 371

Kang, Jerry, 'Cyberspace Privacy: A Proposal Regarding the Private Sector's Processing of Personal Information Generated in Cyberspace', (1998) 50 *Stanford Law Review* 1193

Kang, Jerry, 'Information Privacy in Cyberspace Transactions (1998) 50 *Stanford Law Review* 1193

Kang, Jerry et al, 'Self-Surveillance Privacy' (2012) 97 *Iowa Law Review* 809

Kaplan, Andreas M, and Michael Haenlein, 'Users of the world, unite! The challenges and opportunities of Social Media' (2010) 53 *Business Horizons* 59

Kaplan, Keith B., 'Will virtual courts create courthouse relics?' (2013) 42.2 *Judges Journal* 32

Katyal, Neal, 'Introduction: Disruptive Technologies and the Law' (2014) 102 *Georgetown Law Journal* 1685

Keen, Renee, 'Untangling the Web: Exploring Internet Regulation Schemes in Western Democracies' (2011) 13 *San Diego International Law Journal* 351

Kellow, Philip, 'The Federal Court of Australia: Electronic Filing and the eCourt Online Forum' (2002) 4 *University of Technology Sydney Law Review* 123

Kenny, Coralie and Tahlia Gordon, 'Social media issues for legal practice' (2012) 50(3) *Law Society Journal* 66

Kenyon, Andrew T, 'Not Seeing Justice Done: Suppression Orders in Australian Law and Practice' (2006) 27 *Adelaide Law Review* 279

Keyzer, Patrick et al 'The courts and social media: what do judges and court workers think?" (2013) 25(6) *Judicial Officers' Bulletin* 47

Keyzer, Patrick, 'Media Access to Transcripts and Pleading "Open Justice": A Case Study' (2002) 2(3) *The Drawing Board: An Australian Review of Public Affairs* 209

Keyzer, P, et al, 'The courts and social media: what do judges and court workers think?' (2013) 25(6) *Judicial Officers' Bulletin* 51

Kiel-Chisholm, Scott, 'Catch me if you can: the effective service of bankruptcy documents in a changing world' (2010) 18(4) *Insolvency Law Journal* 197

Kirby, Justice Michael, 'Privacy – in the Courts' (2001) *UNSW Law Journal* 247

Knapp, Keely, '#serviceofprocess@socialmedia: Accepting Social Media for Service of Process in the 21st Century' (2014) 74 *Louisiana Law Review* 337

Koops, Bert-Jaap, 'Law and Technology, and Shifting Power Relations' (2010) 25 *Berkeley Technology Law Journal* 973

Koops, Bert-Jaap, and Ronald Leenes, '"Code" and the Slow Erosion of Privacy' (2005) 12 *Michigan Telecommunications and Technology Law Review* 115

Koops, Bert-Jaap, and Ronald Leenes, 'Privacy regulation cannot be hardcoded. A critical comment on the "privacy by design" provision in data-protection law' (2014) 28 *International Review of Law, Computers & Technology* 159

Kornhauser, Lewis A, 'Governance Structures, Legal Systems and the Concept of Law' (2004) 79 *Chicago-Kent Law Review* 355-381

Krawitz, Marilyn and Justice Howard, 'Should Australian courts give more witnesses the right to Skype?' (2015) 25 *Australian Journal of Judicial Administration* 44

Kreiss, Daniel, 'A vision of and for the Networked Word: John Perry Barlow's *A Declaration of the Independence of Cyberspace* at Twenty' in Barrett James and Niki Strange, *Media Independence Working with Freedom or Working for Free?* (Routledge, 2014)

Kumar, Miiko, 'Keeping Mum: Suppression and Stays in the Rinehart Family Dispute' (2012) 10 *Macquarie Law Journal* 49

Lackey, Michael E Jr, and Joseph P Minta, 'Lawyers and Social Media: The Legal Ethics of Tweeting, Facebooking and Bloggin' (2012) 28 *Touro Law Review* 149

Lange, Patricia G, 'Publicly Private and Privately Public: Social Networking on YouTube' 13 *Journal of Computer-Mediated Communications* 361-380

Lederer, Frederic, I, 'The Road to the Virtual Courtroom? A Consideration of Today's – and Tomorrow's – High Technology Courtrooms' (1999) 50 *South Caroline Law Review* 799

Lederer, Frederic, I, 'The Effect of Courtroom Technologies on and in Appellate Proceedings and Courtrooms (2000) 2 *The Journal of Appellate Practice and Procedure* 25

Ledray, Susan, 'Virtual Services Whitepaper' (February 2013) online, *Harvard Journal of Law & Technology Occasional Paper Series* <http://www.jolt.law.harvard.edu/assets/misc/Ledray-VirtualServices.pdf>

Lee, Laura Whitney, 'Silencing the "Twittering Juror": The Need to Modernize Pattern Cautionary Jury Instructions to Reflect the Realities of the Electronic Age' (2010) 60 *DePaul Law Review* 181

Leenes, Ronald and Bert-Jaap Koops, "'Code": Privacy's Death or Saviour?' (2005) 19 *International Review of Law Computers & Technology* 329

Lessig, Lawrence, 'The Zones of Cyberspace' (1996) 48 *Stanford Law Review* 1403

Lessig, Lawrence, 'The Law of the Horse. What Cyberlaw Might Teach (1999) 113 *Harvard Law Review* 501

Lessig, Lawrence, 'Law Regulating Code Regulating Law' (2003) 35 *Layola University Chicago Law Journal* 1

Libert, Timothy, 'Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on One Million Websites' (2015) 9 *International Journal of Communication* 3544

Lindsay, David, 'Playing Possum? Privacy, Freedom of Speech and the Media Following *ABC v Lenah Game Meats Pty Ltd* Part 11: The Future of Australian Privacy and Free Speech Law, and Implications for the Media' (2002 7 *Media & Arts Law Review* 161

Lindsay, David, 'An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law' (2005) 29 *Melbourne University Law Review* 131

Linke, Anne, and Ansgar Zerfass, 'Social media governance regulatory frameworks for successful online communications' (2013) 17 *Journal of Communication Management* 27

Lipton, Jacqueline D., 'Mapping Online Privacy' (2010) 104(2) *Northwestern University Law Review* 477

Litman, Jessica, 'Information Privacy/Information Property' (2000) 52 *Stanford Law Review* 1283

Lowe, Peter, 'Jury 2.0' (2011) 62 *Hastings Law Journal* 1579

Lusky, L, 'Invasion of Privacy: A Clarification of Concepts' (1972) 72 *Columbia Law Review* 693

McColl, Ruth, 'Privacy, Business and the Digital Era' Address to the New South Wales Law Society Continuing Professional Development Seminar Series, 8 March 2014

McCrudden, Christopher, 'Human Dignity and Judicial Interpretation of Human Rights' (2008) 19 *The European Journal of International Law* 655

McDonald, Barbara, 'Privacy, Princesses, and Paparazzi' (2005-2006) *New York Law School Law Review* 205

McDonald, Barbara, 'A statutory action for breach of privacy: Would it make a (benefical) difference?' (2013) 36 *Australian Bar Review* 241

McLauchlin, Beverly, 'Courts, Transparency and Public Confidence – To the Better Administration of Justice' (2003) 8(1) *Deakin Law Review* 1

Markesinis, Basil et al, 'Concerns and Ideas About the Developing English Law of Privacy (And How Knowledge of Foreign Law Might Be of Help)' (2004) 52 *The American Journal of Comparative Law* 133

Martin, Justice Kenneth Justice, 'Around the nation: Western Australia: Open Justice in Western Australia' (2014) 88 *Australian Law Journal* 779

Marwick, Alice E, and danah boyd, 'I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience' (2010) XX(X) *New Media Society* 1 <http://nms.sagepub.com>

Mason, Rosalind, 'Globalisation of Bankruptcy Practice – An Australian Perspective' (2010) 18 *Insolvency Law Journal* 197

Milivojevic, Sanja and Alyce McGovern, 'The Death of Jill Meagher: Crime and Punishment on Social Media; (2014) 3 *International Journal for Crime, Justice and Social Democracy* 22

Minas, Dilpreet K, 'Enhancing the Legal and Regulatory Environment for Investment in Social Enterprise' (2014) 3(2) *University of Michigan Law School* 257

Moreham, N A, 'Privacy in the Common Law: A Doctrinal and Theoretical Analysis' 2005) 121 *Law Quarterly Review* 628

Moreham, N A, 'Privacy in Public Places' (2006) 65 *Cambridge Law Journal* 606

Morgan, Jonathan, 'Privacy, Confidence and Horizontal Effect: "Hello" Trouble' (2003) 62(2) *Cambridge Law Journal* 444

Morrison, Aimee Hope, 'An impossible future: John Perry Barlow's Declaration of the Independence of Cyberspace' (2009) 11 *New Media & Society* 53

Myers Morrison, Caren, 'Jury 2.0' (2011) 62 *Hastings Law Journal* 1579

Murphy, Richard S, 'Property Rights in Personal Information: An Economic Defense of Privacy' (1996) 84 *The Georgetown Law Journal* 2381

Murray, Andrew and Colin Scott, 'Controlling the New Media: Hybrid Responses to New Forms of Power' (2002) 65 *The Modern Law Review* 491

Nagy, Cate and Emily Rich, 'You can post but you can't hide: *Madden v Seafolly Pty Ltd* and the brave new world of corporate social media' (2014) 17 *Internet Law Bulletin* 74

Nettheim, Garth, 'Open Justice Versus Justice' (1985) 9 *Adelaide Law Review* 487

Nettheim, Garth, 'The Principle of Open Justice' (1984) 8 *University of Tasmania Law Review* 25

Neuberger, Lord, 'Open justice unbound?' (2011) 10 *The Judicial Review* 260

Nicol, Diann et al, 'Time to Get Serious About Privacy Policies: The Special Case of Genetic Privacy' (2014) 42 *Federal Law Review* 149

Nicolas, Ebony, 'A Practical Framework for Preventing "Mistrial by Twitter' (2010) 28 *Cardozo Arts & Entertainment Law Journal* 385

Nissenbaum, Helen, 'Privacy as Contextual Integrity' (2004) 79 *Washington Law Review* 119

Nissenbaum, Helen, 'A Contextual Approach to Privacy Online' (2011) 140 *Doedalus, the Journal of the American Academy of Arts & Sciences* 32

Nissenbaum, Helen, 'From Preemption to Circumvention: If Technology Regulates, Why Do We Need Regulation (and Vice Versa)?' (2011) 26 *Berkeley Technology Law Journal* 1368

Nissenbaum, Helen, 'What is Privacy For?' (2013) 126 *Harvard Law Review* 1904

North, Evan E, 'Facebook Isn't Your Space Anymore: Discovery of Social Networking Websites' (2010) 58 *Kansas Law Review* 179

Ohm, Paul, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 *University of California Los Angeles Law Review* 1701

Ohm, Paul, and James Grimmelmann, 'Dr Generative Or: How I Learned to Stop Worrying and Love the iPhone' (2010) 69 *Maryland Law Review* 910

Oldfather, Chad M, Joseph P Brockhorst and Brian P Dimmer, 'Triangulating Judicial Responsiveness: Automated Content Analysis, Judicial Opinions, and the Methodology of Legal Scholarship' (2012) 64 *Florida Law Review* 1189

O'Reilly, Tim, 'What is Web 2.0 –Design Patterns and Business Models for the Next Generation of Software' (30 September 2005) O'Reilly <http://www.oreilly.com>

O'Reilly, Tim and John Battelle, 'Web Squared: Web 2.0 Five Years On' (October 2009) O'Reilly <http://www.web2summit.com>

Owen, Dave and Caroline Noblet, 'Interdisciplinary Research and Environmental Law' (2014) 41 *Ecology Law Quarterly* 887

Palfrey, John, 'Four Phases of Internet Regulation' (2010) 77 *Social Research*: *An International Quarterly* 981

Pascu, C et al, 'The potential disruptive impact of Internet 2 based technologies' 12(3) *First Monday,* 5 March 2007 <http://firstmonday.org>

Paterson, Nancy E, 'End User Privacy and Policy-Based Networking' (2014) 4 *Journal of Information Policy* 28

Pearce, Robert, 'Privacy, Superinjunctions and Anonymity "Selling My Story Will Sort My Life Out"' (2011) 23 *The Denning Law Journal* 92

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

Pelletier, Robert, 'A New Tort of Privacy: We should be able to sue' (2008) *Law Society Journal* 58

Penner, Roland, 'Access to Justice and Law Reform' (1990) 10 *Windsor Yearbook of Access to Justice* 338

Penny, Johnathon W, 'Privacy and The New Virtualism' (2008) 10 *Yale Journal of Law & Technology* 194

Perry Jr., H.W, 'Access to Justice: Procedure, Polity, and Politics' (2010) 22(3) *Bond Law Review* 189?-211

Pfitzmann, Andreas and Marit Hansen, 'A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management' (10 August 2010) <https://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf> 30-31.

Pilgrim, Timothy, 'Privacy Law Reform: Challenges and Opportunities' (2012) 69 *Australian Institute of Administrative Law Forum* 35

Polden, Mark, 'A New Tort of Privacy: Privacy sounds good, but … ' (2008) *Law Society Journal* 59

Posner, Richard A, A Theory of Negligence' (1972) 1 *Judicial Legal Studies* 29

Plogstedt, Antoinette, 'E-Jurors: A view from the Bench' (2013) 61 *Cleveland State Law Review* 597

Polonetsky, Jules and Omer Tene, 'Privacy and Big Data: Making Ends Meet' (2013) 66 *Stanford Law Review* 25

Ponte, Lucille M, 'The Michigan Cyber Court: A Bold Experiment in the Development of the First Public Virtual Courthouse' (2002) 4 *North Carolina Journal of Law & Technology* 51

Posner, Richard, A., 'The Right of Privacy (1978) 12 *Georgia Law Review* 393

Post, Robert C, 'Three Concepts of Privacy' (2001) 89 *The Georgetown Law Journal* 2087

Preston, Hon Justice Brian J, 'The enduring importance of the rule of law in times of change; (2012) 88 *Australian Law Journal* 175-188

Prosser, William L, 'Privacy' (1960) 49 *California Law Review* 383-423

Ratai, Balzs, 'Understanding Lessig: Implications for European Union Cyberspace Policy' (2005) 19 *International Review of Law, Computers & Technology* 277

Reidenberg, Joel R, 'Governing Networks and Rule-Making in Cyberspace' (1996) 45 *Emory Law Journal* 911

Reidenberg, Joel R, 'Resolving Conflicting International Data Privacy Rules in Cyberspace' (2000) 52 *Stanford Law Review* 1315

Reiling, Dory, 'Doing Justice with Information Technology' (2006) 15 *Information & Communications Technology Law* 189

Reiling, Dory, *Technology for Justice – How Information Technology can support Judicial Reform* (Leiden University Press, 2009

Rhode, Deborah L, 'Access to Justice' (2001) 69(5) *Fordham Law Review* 1785-1819

Richards, Robert D., 'Compulsory Process in Cyberspace: Rethinking Privacy in the Social Networking Age' (2013) 36 *Harvard Journal of Law & Public Policy* 519

Richards, Neil M, 'The Information Privacy Law Project' (2005-6) 94 *Georgetown Law Journal* 1087

Richards, Neil M, and Jonathan H King, 'Three Paradoxes of Big Data' (2013) 66 *Stanford Law Review Online* 41

Robertson, Cassandra Burke, 'The Facebook Disruption: How Social Media May Transform Civil Litigation and Facilitate Access to Justice' (2012) 65 *Arkansas Law Review* 75

Roderick, Sharon, 'Open Justice, the Media and Avenues of Access to Documents on the Court Record' (2006) 29 *University of New South Wales Law Journal* 90

Rodriguez, Philippe-Andre, 'Human dignity as an essentially contested concept' (2015) 28 *Cambridge Review of International Affairs*

Rosen, Jeffrey, 'The Right to Be Forgotten' (2012) 64 *Stanford Law Review Online* 88

Rotenberg, Marc, 'Updating the law of information privacy. The new framework of the European Union' (2013) 362 *Harvard Journal of Law & Public Policy* 605

Roth, Paul, 'Data Protection Meets Web 2.0: Two Ships Passing in the Night' (2010) 33 *UNSW Law Journal* 532-561

Rothman, Jennifer E, 'The Inalienable Right of Publicity' (2012) 101 *Georgetown Law Journal* 185

Rowbottom, Jacob, 'Holding Back the Tide: Privacy Injunctions and the Digital Media' (2017) 133 *Law Quarterly Review* 177

Rubinstein, Ira S., 'Regulating Privacy By Design' (2011) 26 *Berkeley Technology Law Journal* 1409

Russell, Mark, 'Hate sites may affect Bayley's trial' (11 October 2012) *News ABC*

Samuelson, Pamela, 'Privacy as Intellectual Property?' (2000) 52 *Stanford Law Review* 1125

Sarat, Austin, 'Book Review' (1981) 94 *Harvard Law Review* 1911

Sarat, Austin, 'The Litigation Explosion, Access to Justice, and Court Reform: Examining the Critical Assumptions' (1985) 37 *Rutgers Law Review* 319

Scaife, Laura, 'Tweet Revenge? Confusion on Social Media Limits' (2012) 23(3) *Computers & Law Magazine of SCL (Society for Computers and Law)* <http://www.scl.org>

Schauer, Frederick, 'Internet Privacy and The Public-Private Distinction' (1998) 38 *Jurismetrics* 555

Scheb II, John M et al, 'State Trial Courts: A Virtual Future?' (2012) 4 *Baker Center Journal of Applied Public* Policy 58

Schulz, Pamela Dr, 'Trial by Tweet? Social media innovation or degradation? The future and challenge of change for courts' (20120) 22 *Journal of judicial Administration* 29

Schwartz, P.M, 'Internet Privacy and the State' (2000) 32 *Connecticut Law Review* 815

Schwartz, P M, 'Property, Privacy, and Personal Data' (2004) 117 *Harvard Law Review* 2055

Schwartz, P M, 'Prosser's *Privacy* and the German Right of Personality: Are Four Privacy Torts Better than One Unitary Concept?' (2010) 98 *California Law Review* 1925

Schwartz, Paul M., 'The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures' (2013) 126 *Harvard Law Review* 1966

Schwartz, P M, 'Reconciling Personal Information in the United States and European Union' (2014) 102 *California Law Review* 877

Scott, Colin, 'Analysing regulatory space: fragmented resources and institutional design' (2001) *Public Law* 1

Selvadurai, Niloufer, et al 'Identity theft: Aligning law and evolving technologies' (2010) 34 *Criminal Law Journal* 33

Selvadurai, Niloufer, 'The application of criminal defamation to inflammatory comments made on social networking sites: A new role for an old law?' (2012) 36 *Criminal Law Journal* 38

Selvadurai, Niloufer, 'Protecting online information privacy in a converged digital environment – the merits of the new Australian privacy principles', (2013) 23 *Information & Communications Technology Law* 299

Sheehy, Benedict, and Donald Feaver, 'Designing Effective Regulation: A Normative Theory' (2015) 38 *UNSW Law Journal* 392

Simitis, Spiros, 'Reviewing Privacy in an Information Society' (1987) 135 *University of Pennsylvania Law Review* 707

Simitis, Spiros, 'Privacy – An Endless Debate' (2010) 98 *California Law Review* 1989

Small, TW, Robert Boiko and Richard Zorza, 'Designing an Accessible, Technology-Driven Justice System: An Exercise in Testing the Access to Justice Technology Bill of Rights' (2004) 79 *Washington Law Review* 223

Smith, Roger, 'After the Act: what future for legal aid?' (2012) 9(2) *Justice Journal* 8

Snyder, David L., 'Nonparty Remote Electronic Access to Plea Agreements in the Second Circuit' (2009) 35 *Fordham Urban Law Journal* 1263

Solove, Daniel J., "'I've Got Nothing to Hide" and Other Misunderstandings of Privacy' (2008) 44 *San Diego Law Review* 745

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

Solove, Daniel J, 'Access and Aggregation: Public Records, Privacy and the Constitution' (2002) 86 *Minnesota Law Review* 1137

Solove, Daniel J, 'Introduction: Privacy Self-Management and the Consent Dilemma' (2013) 126 *Harvard Law Review* 1880

Solove, Daniel J and Woodrow Hartzog, 'The FTC and the new common law of Privacy' (2014) 114 *Columbia Law Review* 583

Sourdin, Tania, 'Justice and technological innovation' (2015) 25 *Journal of Judicial Administration* 96

Spigelman, James J, 'The Principle of Open Justice: A comparative Perspective' (2006) 29(2) *UNSW Law Journal* 147

Spigelman, James J, 'The Principle of Open Justice: A Comparative Perspective' (2006) 29 *UNSW Law Journal* 147

Stanfield, Allison, 'Cyber Courts: Using the Internet to Assist Court Processes' (1997) 8 *Journal of Law and Information Sciences* 240

Stanfield, Allison and Louise Anderson, 'The Federal Court goes bush' (2001) *Lawyers Weekly* 16

Staudt, Ronald W, 'All the Wild Possibilities: Technology that Attacks Barriers to Access to Justice' (2009) 42 *Loyola of Los Angeles Law Review* 1117

Stepniak, Daniel, 'Why Shouldn't Australian court Procedures be Televised?' (1994) 17 *UNSW Law Journal* 345

Stepniak, Daniel, 'Technology and Public Access to Audio-Visual Coverage and Recordings of Court Proceedings: Implications for common Law Jurisdictions' (2004) 12 *William & Mary Bill of Rights Journal* 819

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

Strahilevitz, Lior Jacob, 'A Social Networks Theory of Privacy' (2005) 72 *University of Chicago Law Review* 919

Strahilevitz, Lior Jacob, 'Towards a Positive Theory of Privacy Law' (2013) 126 *Harvard Law Review* 2010

Sullivan, Clare, 'Digital Citizenship and the Right to Identity in Australia' (2013) 41 *Federal Law Review* 557

Sullivan, Clare, 'The development of digital citizenship in Australia' (2014) *Internet Law Bulletin* 14

Tait, David and Terry Carney, 'Transforming governance and technology in civil and administrative justice' (2013) 22 *Journal of Judicial Administration* 119

Taylor, Greg and David Wright, '*Australian Broadcasting Corporation v Lenah Game Meats:* Privacy, Injunctions and Possums: An analysis of the High Court's Decision' (2020) 26 *Melbourne University Law Review* 707

Tene, Omer, 'Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws' (2013) 74 *Ohio State Law Journal* 1217

Tene, Omer and J Trevor Hughes, 'The Promise and Shortcomings of Privacy Multistakeholder Policy Making: A Case Study' (2015) 55 *Maine Law Review* 437

Tene, Omer, 'Privacy: The new generations' 1 *International Data Privacy Law* 15

Tene, Omer, 'Me Myself and I: Aggregated Disaggregated Identities on Social Networking Services' (2013) 8(3) *Journal of International Commercial Law and Technology* 118

Tene, Omer, and Jules Polonetsky, 'Big Data for All: Privacy and User Control in the Age of Analytics' (2013) 11 *Northwestern Journal of Technology and Intellectual Property* 239

Thierer, Adam, 'The Pursuit of Privacy in a World Where Information Control is Failing' (2013) 36 *Harvard Journal of Law & Public Policy* 409

Thierer, Aman, 'The Perils of Classifying Social Media Platforms as Public Utilities' (2013) 21 *CommLaw Conspectus* 249

Thierer, Adam, 'The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation' (2014) 21 *Richmond Journal of Law & Technology* 1

Thompson, John B, 'Shifting Boundaries of Public and Private Life' (2011) 28 *Theory, Culture & Society* 49

Thomson, Judith Jarvis, 'The Right to Privacy' (1975) 4 *Philosophical and Public Affairs* 323

Tracy, Sarah J, 'Qualitative Quality: Eight "Big-Tent" Criteria for Excellent Qualitative Research' (2010) 16 *Qualitative Inquiry* 837

Tranter, Kieran, 'The Laws of Technology and the Technology of Law' (2011) 20 *Griffiths Law Review* 753

Wagstaff, Emma and Kieran Tranter, 'Taking Facebook at face value: The Refugee Review Tribunal's use of social media evidence' 2014) 21 *Australian Journal of Administrative Law* 172

Walby, Kevin and Alex Luscombe, 'Criteria for quality in qualitative research and use of freedom of information requests in the social sciences' (2016) 1 *Qualitative Research* 1

Walker, Robert Kirk, 'The Right to Be Forgotten' (2012) 64 *Hastings Law Journal* 257

Wallace, Anne, 'Courts on-line: Public Access to the Electronic Court Records' (2000) 10 *Journal of Judicial Administration* 94

Wallace, Anne, 'Virtual Justice in the Bush: The Use of Court Technology in Remote and Regional Australia' (2008) 19 *Journal of Law, Information and Science* 1

Wallace, Anne, Deborah Blackman and Emma Rowden, 'Reconceptualizing Security Strategies For Courts: Developing A Typology For Safer Court Environments' (2013) 5(2) *International Journal For Court Administration* 3

Warren, Marilyn, Chief Justice, 'Open Justice in the Technological Age' (2013) remarks on the occasion of the 2013 Redmond Barry lecture 40 *Monash University Law Review* 50

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

Waz, Joe, and Phil Weiser, 'Internet Governance: The Role of Multistakeholder Organizations' (2012) 10 *Journal on Telecommunications and High Technology Law* 331

Westin, Alan F, 'Social and Political Dimensions of Privacy' (2003) 59 *Journal of Social Issues* 3

Westin, Alan F, 'Science, Privacy, and Freedom: Issues and Proposals for the 1970's: Part 11 – Balancing the Conflicting Demands of Privacy, Disclosure, and Surveillance' (1966) 66 *Columbia Law Review* 1205

Westerman, David et al, 'Social Media as Information Source: Recency of Updates and Credibility of Information' (2014) 19 *Journal of Computer-Mediated Communication* 171

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

Widdison, Robin, 'Electronic Paths to Justice;, (2003) 2 *The Journal of Information, Law and Technology* <http://elj.warwick.ac.uk/jilt/03-2/widdson.html>

Willheim, Ernst, 'Are Our Courts Truly Open? (2002) 13 *Public Law Review* 191

Wilson, Nigel, 'Regulating the information age – How will we cope with technological change?' (2010) 33 *Australian Bar Review* 119

Witzleb, Norman, '"Personal Information" under the Privacy Act 1988 (Cth) – Privacy Commissioner v Telstra Corporation Ltd [2017] FCAFC 4' (2017) 45 *Australian Business Law Review* 188

Wolf, Michael J, 'Collaborative Technology Improves Access to Justice' (2012) 15 *New York University Journal of Legislation and Public Policy* 759

Wu, Tim, 'When Code Isn't Law' (2003) 89 *Virginia Law Review* 679

Xu, Heng, 'Reframing Privacy 2.0 in Online Social Networks' (2012) 14 *University of Pennsylvania Journal of Constitutional Law* 1077

Yeung, Karen, 'Can We Employ Design-Based Regulation while Avoiding *Brace New World*?' (2011) 3 *Journal of Law, Innovation and Technology* 1

Zic, Timothy, 'Space, Place, and Speech: The Expressive Topography' (2005) The Social Science Research Network Electronic Paper Collection <http://ssrn.com>

Zimmeck, Sebastian, 'The Information Privacy Law of Web Applications and Cloud Computing' 29 *Santa Clara Computer & High Technology Law Journal* 451

Zimmer, Michael, 'The Externalities of Search 2.0: The Emerging Privacy Threats when the Drive for the Perfect Search Engine meets Web 2.0' (3 March 2008) 13(3) *First Monday* <http://dx.doi.org/10.5210/fm.v13i3.2136>

Zittrain, Jonathan L, 'The Generative Internet' (2005) 119 *Harvard Law Review* 1975

Zittrain, Jonathan, 'Privacy 2.0' (2008) 66 *University of Chicago Legal Forum* 65

Zora, Marcy, 'The Real Social Network: How Jurors' Use of Social Media and Smart Phones Affects a Defendant's Sixth Amendment Rights' (2012) *University of Illinois Law Review* 609

Zorza, Richard, 'Courts in the 21st Century: The Access to Justice Transformation' (2010) 49 *The Judges' Journal* 14

Zorza, Richard, and Donald J Horowitz, 'The Washington State Access to Justice Principles: A Perspective for Justice System Professionals' (2006) 27 *The Justice System Journal* 248

Zumbansen, Peer, 'The Ins and Outs of Transnational Private Regulatory Governance: Legitimacy, Accountability, Effectiveness and a New Concept of "Context"' (2012) 13 *German Law Journal* 1269

B *Books*

Anderson, Chris, *The Long Tail: Why the Future of Business is Selling Less of More* (Hyperion Books, 2009)

Australian Institute of Judicial Administration Incorporated, *Australian Courts: Serving Democracy and its Publics* (The Australian Institute of Judicial Administration Incorporated, 2013)

Baker, J H, *The Legal Profession and the Common Law: Historical Essays* (Hambledon Press, 1986)

Benkler, Yochai, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (Yale University Press 2006)

Bentham, Jeremy, *The Works of Jeremy Bentham* Vol 6 Chapter X, 'Of Publicity and Privacy, as applied to Judicature in General, and to The Collection of the Evidence in Particular' (published under the Superintendence of his Executor, John Bowring, Edinburgh: William Tait, 1838-1843)

Bingham, Tom, *The Rule of Law* (Penguin Books, 2011)

Brin, David, *The Transparent Society. Will Technology Force us to Choose Between Privacy and Freedom?* (Perseus Books Group, 1998)

Brownsword, Roger, *Rights, Regulation and the Technological Revolution* (Oxford University Press, 2008)

Brownsword, Roger and Morag Goodwin, *Law and the Technologies of the Twenty-First Century* (Cambridge University Press, 2012)

Brunton, Finn and Nissenbaum, Helen, *Obfuscation: A User's Guide for Privacy and Protest* (The MIT Press, 2015)

Bygrave, Lee A, *Data Privacy Law* (Oxford University Press, 2014)

Cane, P, and H Kritzers (eds), *The Oxford Handbook of Empirical Legal Research* (Oxford University Press, 2010)

Christensen, Clayton, *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail* (Harvard Business Review Press, 1997)

Coke, Edward, *The Second Part of the Institutes of the Laws of England: Containing the Exposition of Many Ancient And Other Statues* (Printed for E and R Brooke, Bell-Yard, near Temple Bar, 1797)

Cowen, Professor Zelman, *The Private Man: The Boyer Lectures 1969* (The Australian Broadcasting Commission, 2001)

Dayton, Adrian, *Social Media for Lawyers*: *Twitter Edition* (Ark Group, 2009)

Denning, Sir Alfred, *The Road to Justice* (Stevens & Sons, 1955)

Eltis, Karen, *Courts, Litigants and the Digital Age* (Irwin Law Inc., 2012)

Fukuyama, Frances, *Our Posthuman Future* (Profile Books, 2002)

Fitzgerald, B and Anne Fitzgerald, Gaye Middleton, Eugene Clark, Yee Fen Lim, *Internet and E-Commerce Law, Business and Policy* (Lawbook Co., 2011)

Floridi, Luciano, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality* (Oxford University Press, 2014)

Fuster, Gloria Gonzalex, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer, 2014)

Genn, Dame Hazel, *Judging Civil Justice (The Hamlyn Lectures, 2008)* Cambridge University Press, 2010)

Gerring, John, *Case Study Research: Principles and Practices* (Cambridge University Press, 2007)

Goldsmith, Jack and Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World* (Oxford University Press, 2006)

Hart, H L A, *Essays on Bentham* (Clarendon Press, 1982)

Hart, H L A, *The Concept of Law* (Clarendon Press, 1961: 2nd ed 1994)

Hildebrandt, Mireille, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Edward Elgar Publishing, 2015)

Hildebrandt, Mireille, *A Vision of Ambient Law*: *Regulating Technologies* (Hart, 2008)

Huberman, A Michael, and Matthew B. Miles, *The Qualitative Researcher's Companion* (Sage Publications, 2002)

Hutchinson, Terry, *Researching and Writing in Law* (Lawbook Co, 3rd ed, 2010)

Jaconelli, Joseph, *Open Justice: A critique of the Public Trial* (Oxford University Press, 2002)

Kenyon, Andrew T and Megan Richardson, *New Dimensions in Privacy Law International and Comparative Perspectives* (Cambridge University Press, 2006)

Klang, Mathias, *Disruptive Technology: effects of technology regulation on democracy*, Volume 36 Göthenburg studies in informatics (Göteborg University, 2006)

Lambert, Paul, *Courting Publicity: Twitter and Television Cameras in Court* (Bloomsbury Professional, 2011)

Lessig, Lawrence, *Code and other Laws of Cyberspace* (Basic Books, 1999)

Lessig, Lawrence, *Code: Version 2.0* (Basic Books, 2006)

Mitchell, William *Me++: The Cyborg Self and the Networked City* (The MIT Press, 2004)

Munir, A and S Yasin, *Privacy and Data Protection: A Comparative Analysis with Special Reference to the Malaysian Proposed Law* (Sweet & Maxwell, 2002)

Neuman, W Lawrence, *Social Research Methods: Qualitative and Quantitative Approaches* (Allyn & Bacon, 2000, 4th ed)

Nissenbaum, Helen, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press, 2010)

Packard, Ashley, *Digital Media Law* (Wiley-Blackwell, 2nd ed, 2013)

Parker, Stephen, *Courts and the Public* (Australian Institute of Judicial Administration Incorp., 1998)

Parker, Christine et al, '*Regulating Law'* (Oxford University Press, 2004)

Parkinson, Patrick, *Tradition and Change in Australian Law* (5th ed Thomson Reuters, 2013)

Puschmann, Cornelius and Jean Burgess, 'The Politics of Twitter Data' *Twitter and Society* (Peter Lang Publishers, 2013)

Richardson, Janice, *Law and the Philosophy of Privacy* (Routledge, 2016)

Saldaña, Johnny, *The Coding Manual for Qualitative Researchers* (Sage Publications Ltd, 3rd ed, 2016)

Scaife, Laura, *Handbook of Social Media and The Law* (Routledge, 2015)

Schulz, Pamela D, *Courts and Judges on Trial – Analysing and Managing the Discourses of Disapproval* (Transaction Publishers, 2010)

Scott, Colin, *Regulation* (Ashgate/Dartmouth, 2003)

Searle, John R, *The Construction of Social Reality*, (Free Press, 1995)

Solove, Daniel J, *the digital person: Privacy and Technology in the Information Age* (New York University Press, 2004)

Solove, Daniel, J, *the future of reputation: gossip, rumor, and privacy on the internet* (Yale University Press, 2007)

Solove, Daniel J, *Nothing to Hide: The False Tradeoff Between Privacy and Security* (Yale University Press, 2011)

Stephenson, Neal, *The Diamond Age,* (Bantam Spectra Book, 1995)

Stephniak, Daniel, *Audio-Visual Coverage of Courts* (Cambridge University Press, 2008)

Sullivan, Clare, *Digital Identity: An Emergent Legal Concept* (University of Adelaide Press, 2011)

Susskind, Richard E, *The End of Lawyers? Rethinking the Nature of Legal Services* (Oxford University Press, 2008)

Wacks, Raymond, *Privacy and Media Freedom* (Oxford University Press, 2013)

Walzer, Michael, *Spheres of Justice: A Defense of Pluralism* (Basic Books, 1983)

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

Whitaker, Reg, *The End of Privacy: how total surveillance is becoming a reality* (The New Press, 1999)

Windeyer, W J V, *Legal History* (2nd ed, Law Book Company of Australasia, 1957),

Witzleb, Normann, David Lindsay, Moira Paterson and Sharon Rodrick, *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge University Press, 2014)

Woolf, Sir Harry, *Access to Justice: Final Report to the Lord Chancellor on the Civil Justice System in England and Wales* (*Wolf Report*) (Her Majesty's Stationery Office, 1996)

Wu, Tim, *The Master Switch: The Rise and Fall of Information Empires* (Atlantic Books, 2010)

Zittrain, Jonathan L, *The Future of the Internet and How to Stop It* (Yale University Press, 2008)

C *Edited books*

Allars, Margaret, 'Cross-Border Transfer of Personal Information: Evolving Privacy Regulation in Europe and Australia' 106-125 in Dieter Dorr (ed) *Media Convergence: Perspective on Privacy* Vol 9 (De Gruyter, 2014)

Augenanger, Stefan and Dieter Dorr, Stephan Fussel, Oliver Quiring and Karl N Renner (eds), *Media Convergence: Perspectives on Privacy* (2014) Vol 9

Butler, Susan (ed), *Macquarie Dictionary* (Macquarie Dictionary Publishers Pty Ltd, 6th ed, 2013).

Brownsword, Roger, (ed) *Global Governance and the Quest for Justice* Vol IV: Human Rights 'Introduction: Global Governance and Human Rights' (Hart Publishing, 2004)

Cappelletti, Mauro, and Bryant Garth (eds) Volume 1: A World Survey, *Access to Justice* (Dott AGiuffre, 1978)

Cheung, Anne S Y, and Rolf Weber (eds) *Privacy and Legal Issues in Cloud Computing* (Edward Elgar Publishing, 2015)

Fitzgerald, Brian (ed) *Access to Public Sector Information: Law Technology & Policy* (Sydney University Press, 2010)

Friedman, Lawrence, 'Access to Justice: Social and Historical Context' (1978) in M Cappelletti and J Weisner. Milan, Dott. A Giuffre (eds) II 3

Gruen, Nicholas 'Engage: Getting on With Government 2.0' in Fitzgerald, Brian (ed) *Access to Public Sector Information: Law, Technology & Policy* (Sydney University Press, 2010)

Guibault, Lucie and P Bernt Hugenholtz (eds) *The future of the public domain* (Kluwer Law International, 1960)

Keyzer, Patrick, Jane Johnson and Mark Pearson (eds) *The Courts and the Media: Challenges in the Era of Digital and Social Media* (Halstead Press, 2007)

Martínez, Agustí Cerrillo I and Pere Fabra I Abot (ed), *E-Justice: Information and Communication Technologies in the Court System* (Information Science Reference, 2009)

Max, Gary T, 'Forward' in David Wright et al (eds) *Safeguards in a World of Ambient Intelligence* (Springer, 2008)

Palmer, Ellie et al (eds) *Access to Justice: Beyond the Policies and Politics of Austerity* (Hart Publishing, 2016)

Piscuzzi, Giovanni, Umberto Izzo and Matteo Maalotti (eds) *Comparative issues in Governance of Research Biobanks: Property, Privacy, Intellectual Property, and the Role of Technology* (Springer, 2013)

Ritchie, Jane and Liz Spencer, 'Qualitative Data Analysis for Applied Policy Research' in A Michael Huberman, Matthew B Miles (eds) *The Qualitative Researcher's Companion* (Sage Publications, 2002)

Sartor, Giovannit et al (eds) *Approaches to Legal Ontologies: Theories, Domains, Methodologies* Law, Governance and Technology Series (Springer, 2011)

Wang, Yang and Alfred Kobsa, 'Privacy-Enhancing Technologies' Chapter XIII in Manish Gupta and Raj Sharman (eds) *Handbook of Research on Social and Organizational Liabilities in Information Security* (Information Science Reference, 2009)

Wrbka, Stefan, Steven Van Uytsel and Mathias Siems (eds), *Collective Actions: Enhancing access to justice and reconciling multilayer interests?* (Cambridge University Press, 2012)

D *Chapters in edited books*

Baker, John Hamilton, 'The Changing Concept of a Court' Chapter 10 in *The Legal Profession and the Common Law: Historical Essays* (Hambleton Press, 1986)

Berg, Bruce L., and Howard Lune, *Qualitative Research Methods for the Social Sciences* (Peachpit Press, 2011) 8th ed. Chapter 11, 'An Introduction to Content Analysis

Berg, Bruce L and Howard Lune, 'An Introduction to Content Analysis' Chapter 11 in *Qualitative Research Methods for the Social Science,* (Peachpit Press, 8th ed, 2011)

Berg, B van den, and S Pötzsch, RE Leenes, K Borcea-Pfitzmann and F Beato, 'Privacy in Social Software' Chapter 2 in *Privacy and identity management for life* (Springer, 2011)

Braithwaite, John, and Christine Parker, 'Conclusion' in *Regulating Law* (Oxford University Press, 2004) 273

Davies, Simon G, 'Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity' in *Technology and Privacy: The New Landscape* Agre, Philip E., and Mar Rotenberg (The MIT Press, 1997)

Döhmann, Indra Spiecher genannt, 'The European Approach towards Data Protection in a Globalized World of Data Transfer' in *Media Convergence: Perspectives on Privacy* Stefan Augenanger et al (eds) (de Gruyter, 2014)

Mireille Hildebrandt, 'Location Data, Purpose Binding and Contextual Integrity: What's the Message?' Chapter 3 in L Floridi (ed) *Protection of Information and the Right to Privacy – A New Equilibrium?* (Springer International Publishing, 2014)

Galligan, D J, 'Legal Theory and Empirical Research' in Peter Casne and Herbert M Kritzer (eds.) *The Oxford Handbook of Empirical Legal Research* (Oxford University Press, 2010)

Gruen, Nicholas, 'Engage: Getting on With Government 2.0' Vol 2 Chapter 28 in Brian Fitzgerald (ed) *Access to Public Sector Information: Law, Technology & Policy* (Sydney University Press, 2010)

Johnston, Jane, 'Courts' New Visibility 2.0', 41 in *The Courts and the Media – Challenges in the Era of Digital and Social Media* (Halstead Press, 2007)

Kenyon, Andrew T and Megan Richardson, 'New dimensions in privacy: Communications technologies, media practices and law', Chapter 1 in Andrew T Kenyon and Megan Richardson (eds) *New dimensions in privacy: International and Comparative Perspectives* (Cambridge University Press, 2010)

Keyzer, Patrick, 'Who Should Speak for the Courts and How? The Courts and the Media Today in Patrick Keyzer, Jane Johnston and Mark Pearson (eds) *The Courts and the Media: Challenges in the Era of Digital and Social Media'* (Halstead Press, 2012)

Kong, Joe, Xiaoxi Fan and K P Chow, 'Introduction to cloud computing and security issues, Chapter 1 in Anne S Y Cheung and Rolf H Weber (eds), *Privacy and Legal Issues in Cloud Computing* (Edward Elgar, 2015)

O'Reilly, Tim, 'Not 2.0?' (5 August 2005) <http://radar.oreilly.com/2005>

O'Reilly, 'Open Data and Algorithmic Regulation' Chapter 22 in Brett Goldstein and Lauren Dyson (eds) *Beyond Transparency: Open Data and the Future of Civic Innovation* (Code for America Press, 2013)

Patching, Roger, 'The *News of the World* Scandal and the Australian Privacy Debate' Chapter 12 in Patrick Keyzer, Jane Johnston and Mark Pearson (eds) *The Courts and the Media: Challenges in the Era of Digital and Social Media* (Halstead Press, 2007)

Ritchie, Jane and Liz Spencer, 'Qualitative Data Analysis for Applied Policy Research' in A Michael Huberman and Matthew B Miles (eds) *The Qualitative Researcher's Companion* (Sage Publications, 2002)

Roosendaal, Arnold, 'We Are All Connected to Facebook…by Facebook!' 3-19 in S. Gutwirth et al (eds) *European Data Protection: In Good Health?* (2012, Springer)

Sage-Jacobson, Susannah, 'The Ongoing Search for a Demand-Side Analysis of Civil Justice in Australia', Chapter 5 in *Australian Courts: Servicing Democracy and its Publics*, The Australasian Institute of Judicial Administration Incorporated, Melbourne, 2013)

Sandefur, Rebecca L, 'Access to Justice: Classical Approaches and New Directions' ix in Rebecca L Sandefur (ed) *Access to Justice: Sociology of Crime, Law, and Deviance* Vol 12 (Emerald/JAI Press, 2009)

Stepniak, Daniel, 'Cameras in Court: Reluctant Admission to Proactive Collaboration' in Kayzer, P, J Johnston and M Pearson (eds) *The Courts and the Media – Challenges in the Era of Digital and Social Media* (Halstead Press, 2012)

Vickery, Graham, 'Foreword', in Brian Fitzgerald (ed), Vol 2, *Access to Public Sector Information: Law, Technology & Policy* Vol 2 (Sydney University Press, 2010)

Webley, Lisa, 'Qualitative Approaches to Empirical Legal Research' in Peter Cane and Herbert M Kritzer (eds) *The Oxford Handbook of Empirical Legal Research* (Oxford University Press, 2010)

E *Reports*

Advisory Council to Google, *Right to be Forgotten* (Report, 6 February 2015) <https://www.google.com/advisorycouncil/>

Agrast, Mark D et al, *The World Justice Project: Rule of Law Index 2012-2013* (Research Report, World Justice Project, 2013) <https://worldjusticeproject.org/our-work/wjp-rule-law-index>

Arnold, Bruce et al, Australian Privacy Foundation (Submission No 110 to the Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era,* 15 November 2013

Attorney General's Department, Australian Government, *A Strategic Framework for Access to Justice in the Federal Civil Justice System* (Report, Access to Justice Taskforce, 30 September 2009)

Australian Attorney-General's Department, *Productivity Commission Inquiry into Access to Justice Arrangements* (Submission, Australian Government, November 2013) <http://www.ag.gov.au>

Australian Auditor-General, *Cyber Attacks: Securing Agencies, ICT Systems: Across Agencies* Audit Performance Report, No 50 2013-14, Australian National Audit Office, 24 June 2014) <https://www.anao.gov.au/work/performance-audit/cyber-attacks-securing-agencies-ict-systems>

Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice,* Report No 108 (2008) Vol 2

Australian Law Reform Commission, *Privacy*, Report No 22 (1983)

Australian Law Reform Commission, *Unfair Publication: Defamation and Privacy*, Report No 11 (1979)

Barendrecht, Maurits, Peter Kamminga and Jin Ho Verdonschot, *Priorities for the Justice System: Responding to the Most Urgent Legal Problems of Individuals* (Tilburg University Legal Studies Working Paper Series on Civil Law and Conflict Resolution Systems, No 001/2008 and No 002/2008, Tilburg University, Tilburg Institute for Interdisciplinary Studies of Civil Law and Conflict Resolution Systems, International Victimology Institute Tilburg, Tilburg Law and Economics Centre, Hague Institute for the Internationalisation of Law, 5 February 2008)

Cyberlaw Clinic, *Best Practices in the Use of Technology to Facilitate Access to Justice Initiatives* (Preliminary Report, Berkman Center for Internet & Society at Harvard University, July 30, 2010) <https://cyber.harvard.edu/publications/2010/Best_Practices_Technology_Access_to_Justice>

Conference of Court Public Information Officers, *2014 CCPIO New Media Survey,* (Report, Conference of Court Public Information Officers, National Center for State Courts and The E W Scripps School of Journalism at Ohio University (6 August 2014) <http://www.ccpio.org>

Dunn, Meghan A, *Jurors' Use of Social Media During Trials and Deliberations: A Report to the Judicial Conference Committee on Court Administration and Case Management* (Report, Federal Judicial Center, 22 November 2011)

Dunn, Meghan A, *Jurors' and Attorneys' Use of Social Media During Voir Dire, Trial, and Deliberations: A Report to the Judicial Conference Committee on Court Administration and Case Management*, (Report, Federal Judicial Center, 1 January 2014) <https://fjc.gov>

Edelman, Richard, *The Power of the Earned Brand* (Report, Edelman, 23 June 2015) <http://www.edelman.com>

DeNardis, Laura, *The Emerging Field of Internet Governance* (Working Paper, Yale Information Society, 2010) <http>//ssrn.com>

Gasser, Urs, Faris, Robert and Rebekah Heacock, *Internet Monitor 2013: Reflections on the Digital World* (Research Publication No 2013-27, Harvard University – Berkman Klein Center for Intrent & Society, 12 December 2013) <https://clinic.cyber.harvard.edu/publication/internet-monitor-reflections-on-the-digital-world-2/>

Grainger, Julie, *Litigants in Person in the Civil Justice System – learning from NZ, the US and the UK* (Report, prepared for The Winston Churchill Memorial Trust of Australia (1 November 2013)

Gramatikov, Martin, and Laxminarayan, Malini, *Weighting Justice: Constructing an Index of Access to Justice* (Working Papter, Tilburg University Legal Studies, 16 February, 2008) <http://www.hiil.org/publication/weighting-justice-constructing-an-index-of-access-to-justice>

Her Majesty's Courts Service, *Confidence and confidentiality: Improving transparency and privacy in family courts*, (Report, No CP(R)11/06, Department for Constitutional Affairs, Justice, rights and democracy, 22 March 2007) <https://www.gov.uk>

IBM, *The business value of Web 2.0 technology: IBM's vision for tapping the collective knowledge of the extended value chain* (Report, IBM Corporation, 2007) <http://www.ibm.com/web20>

Information Commissioner's Office, *The Guide to Data Protection* (Report, 26 November 2008) <https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/>

Johnston, Jane et al, *Juries and Social Media: A Report Prepared for the Victorian Department of Justice,* (Report, The Standing Council on Law and Justice, 6 January 2013)

Judges Technology Advisory Committee, *Open Courts, Electronic Access to Court Records, and Privacy* (Discussion Paper prepared on behalf of the Judges Technology Advisory Committee for the Canadian Judicial Council, (May, 2003) <https://www.cjc-ccm.gc.ca>

Kelleher, Denis, 'EU Data Protection Law; The First 25 Years' (5 November 2015 *Privacy Perspectives* <http://www.iapp.org>

Koops, Bert-Jaap, *Ten Dimensions of Technology Regulation – Finding Your Bearings in the Research Space of an Emerging Discipline* (Working Paper, No 015/2010, Tilburg University, 2010)

Krawitz, Marilyn, *Guilty as Tweeted: Jurors Using Social Media Inappropriately During the Trial Process* (Research Paper No 2012-01, University of Western Australia, Faculty of Law, 16 November 2012)

KRDP Kantor Ltd and Centre for Public Reform, *Comparative Study on Different Approaches to New Privacy Challenges, in particular in the light of technological developments'* (Final Report, No JLS/2008/C4/001-30-CE-0219363/00-28, European Commission, Directorate-General Justice, Freedom and Security, 20 January 2010) <http://ec.europa.eu/justice/data-protection/document/studies/index_en.htm>

Kruger, Leonard G, *The Future of Internet Governance: Should the U.S. Relinquish Its Authority Over ICAAN?* (Report, Congressional Research Service, 5 May 2015) <http://www.crs.gov>

La Rue, Frank, Special Rapporteur, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,* UN Doc A/HRC/17/27 (16 May 2011)

Legal Projects Team, *The Impact of Online Social Networking on the Legal Profession and Practice* (Report, International Bar Association, February 2015) <http://www.ibanet.org>

Leveson, Lord Justice, *The Leveson Inquiry: An Inquiry Into The Culture, Practices and Ethics of the Press* (Report, No 0780 2012-13, House of Commons, United Kingdom, 29 November 2012) <http://webarchive.nationalarchives.gov.uk/20140122145147/http://www.official-documents.gov.uk/document/hc1213/hc07/0780/0780.asp>

McKinsey Global Institute, *Big data: The next frontier for innovation, competition, and productivity* (Report, McKinsey & Company, May 2011) <http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-the-next-frontier-for-innovation>

Managing Justice, *An evidence base for the federal civil justice system* (Report, Access to Justice Division Attorney-General's Department, February 2011) <http://www.managingjustice.com.au>

Martindale-Hubble, *Global Social Media Check Up: A global audit of law firm engagement in social media methods* (Report, LexisNexis Martindale-Hubbell, in association with Bruson-Marsteller, 2011) <http://www.martindale-hubbell.co.uk/socialmedia>

Myers Morrison, Caren, *Privacy, Accountability, and the Cooperating Defendant: Towards a New Role for Internet Access to Court Records'* (Public Law & Legal Theory Working Paper, No 99, New York University School of Law, 23 September 2009)

New Media Committee, *New Media and the Courts: The Current Status and A Look at the Future* (Report, Conference of Court Public Information Officers, 26 August 2010) <http://www.ccpio.org>

New South Wales Law Reform Commission, *Invasion of Privacy*, Report 120 ( )

Perrin, Andrew, *Social Media Usage: 2005-2015* (Report, Pew Research Center, October 2015) <http://www.pewinternet.org>

Roberts, Chief Justice, *2014 Year-End Report on the Federal Judiciary* (Report, Public Information Office, United States Supreme Court, 31 December 2014) <http://www.supremecourt.gov>

Robinson, N et al, *Review of the European Data Protection Direction,* (RAND Europe Report, Information Commissioner's Office, UK May 2009)

Rolph, David, *Politics, Privacy and the Public Interest: A Case Study from Australia* (Research Paper, No 12/38, Sydney Law School, 2012) <http://ssrn.com>

Rubinstein, Ira S., *Big Data: The End of Privacy or a New Beginning?* (Working Paper, No 12-56, New York University School of Law, Public Law & Legal Theory Research Paper Series (October 2012)

Rolph, David, *Politics, Privacy and the Public Interest: A Case Study from Australia'* (Research Paper, No 12/38, Sydney Law School, 1 May 2012) <http://ssrn.com/abstract=2070443>

Sherman, Jo and Allison Stanfield, *eCourt Integration Strategy Final Report* (Report, eLaw, January 2004) <http://www.elaw.com.au>

Sensis, *Yellow Social Media Report: What Australian people and businesses are doing with social media*, (Report, Sensis, May 2014) <https://sensis.com.au>

Sensis, *How Australian people and businesses are using social media* (Report, Sensis, May 2015) <www.sensis.com.au/socialmediareport>

Soltani, Ashkan, 'The Privacy Puzzle: Little or No Choice', 81-82, 81 in *Internet Monitor 2013: Reflections on the Digital World,* (Research Publication, No 2013-27, The Berkman Center for Internet & Society at Harvard University, 11 December 2013) <https://cyber.harvard.edu/research/internet_monitor/paper_series>

Standing Committee on Access to Justice, *Access to Justice Metrics: Envisioning Equal Justice* (Discussion Paper, Canadian Bar Association, April 2013) <http://www.cba.org/CBA-Equal-Justice/Resources/Reports-Discussion-Papers>

Victorian Law Reform Commissions, *Surveillance in Public Places,* (Report No 18)

Young, Jamie, *A Virtual Day in Court: Design Thinking & Virtual Courts* Report, Royal Society for the encouragement of Arts, Manufactures and Commerce (*RSA*), December, 2011) <https://www.thersa.org>

F *Cases*

Australian Olympic Committee Inc v Big Fights Inc [1999] FCA 1042

AAW15 v Minister for Immigration & Anor [2015] FCCA 663

AB Limited, JW, SM and CM v Facebook Ireland Limited and A Person or Persons Adopting the Pseudonyms Ann Driver and Alan Driver [2013] NIQB 14

ACCC v Air New Zealand Limited (No 4) [2012] FCA 1439

Attorney General v Fraill [2011] EWCA Crim 1570

American Express Australia Ltd v Michaels (2010) 237 FLR 268

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

Arrington v DaimlerChrysler Corp 109 Ohio St.ed 539

Assistant Commissioner Condon v Pompano Pty Ltd (2013) 252 CLR 38

Australian Competition and Consumer Commission v Allergy Pathway Pty Ltd and Anor No 2 (2011) 192 FCR 34

Attorney-General v Leveller Magazine [1979] AC 450

Bianca Hope Rinehart v Georgina Hope Rinehart [2014] FCA 1241

Strauss v Police (2013) 115 SASR 90

Bustillo v Hilliard 16 Fed. Appx, 494

Byrne & Howard (2010) 239 FLR 62

Capital Pty Ltd v Corbo & Poyser (unreported, ACT Supreme Court, Master Harper, 12 December 2008)

Citygroup Pty Limited v Weerakoon [2008] QDC 174

Coco v A.N. Clarke (Engineers) Limited [1969] RPC 41

Commonwealth v Werner 81 Mass App Ct 689

Davis & Ors v Secretary of State for the Home Department & Ors [2015] EWHC 2092

Dennis v United States (1951) 341 US 494

Department of Air Force v Rose, 480 US 749

Dickason v Dickason (1913) 17 CLR 50

Douglas v Hello! [2001] QB 967

Dover-Ray v Real Insurance Pty Ltd (2010) 204 IR 399

Essendon Football Club v Chief Executive Officer of the Australian Sports Anti-Doping Authority (2014) 227 FCR 1

Evans v Amicus Healthcare Ltd [2004] EWCA Div 727

Evans v Amicus Healthcare Ltd and others [2003] EWHC 2161 (Fam)

Evans v United Kingdom [GC] No 6339/05, § 77, ECHR 2007-IV 96, 237-43

Google Spain SL, Google Inc. v Agencia Española de Protection de Datos (AEPD), *Mario Costeja González* (Case C-131/12) (13 May 2014)

Harman v Home Office [1983] 1 AC 280

Hogan v Australian Crime Commission (2010) 240 CLR 651

Hogan v Hinch (2011) 243 CLR 506

Haruna v The Queen (2013) 278 FLR 194

Helow v Scotland (AG) [2008] 2 All ER 1031

John Fairfax & Police Tribunal of New South Wales (1986) 5 NSWLR 465

John Fairfax Publications Pty Ltd v District Court of New South Wales (2004) 61 NSWLR 344

Lukazsewski v Capones Pizzeria Kyneton [2009] AIRC 280

McAlpine v Bercow [2013] EWHC 1342

McPherson v McPherson [1936] AC 177

Marsh v Baxter (2014) 46 WAR 377

MKM Capital Pty Ltd v Corbo & Poyser (Unreported, ACT Supreme Court, Master Harper, 12 December 2008)

Minister for Immigration and Citizenship v SZRKT (2013) 212 FCR 99

MZADZ v Minister for Immigration & Anor [2015] FCCA 1589

National Rugby League Investments Pty Limited v Singtel Optus Pty Ltd (2012) 201 FCR 147

News Digital Media Pty Ltd v Mokbel (2010) 30 VR 248

Norwest Holst Ltd v Department of Trade [1978] Ch 201

Own Motion Investigation v Bankruptcy Trustee Firm [2007] PrivCmrA 5

People v Fernino, 851 NYS 2d 339 (13 February 2008)

People v McNeely, No D048692, 2007 WL 1723711, at *2 (Cal. Ct. App. June 14, 2007)

Prince Albert v Strange (1849) 47 ER 1302

Privacy Commissioner v Telstra Corporation Limited [2017] 262 IR 230

Purvis v Commissioner of Social Security No 09-5318 (SDW) (MCA) 2011 (D.N.J. Feb 23, 2011)

R *(Guardian News & Media Ltd) v City of Westminster Magistrates Court* [2012] EWCA Civ 420

R *(on the application of Davis MP) v Secretary of State for the Home Department (Open Rights Group and ors intervening)* [2017] 1 All ER 62

Re Applications by Chief Commissioner of Police (Vic) (2004) 9 VR 275

Re ML (Use of Skype Technology) [2013] EWHC 2091 (Fam)

Re Todd; Ex parte Todd (1986) 68 ALR 483

R v Dupas (No 3) (2009) 28 VR 380

R v Karakaya [2005] Cr App R 5

R v Marsland (Unreported, Supreme Court of New South Wales, Court of Appeal, Gleeson CJ, Lee CJ at Cl, Hunt J, 17 July 1991)

Re Applications by Chief Commissioner of Police (Vic) (2004) 9 VR 275

Rezaeipoor v Arbbalvai [2012] EWHC 146 (Ch)

RJW & SJW v The Guardian newspaper & Person and Persons Unknown (Claim no HQ09)

Rinehart v Welker [2011] NSWCA 403

Rinehart v Welker [2011] NSWCA 345

Rinehart v Rinehart (2014) 320 ALR 195

Russell v Russell (1976) 134 CLR 495

Seafolly Pty Ltd v Madden (2012) 297 ALR 337

Scott v Scott [1913] AC 473

Seven Network Limited v News Limited [2007] FCA 1062

SmithKline Becham Biologicals SA v Connaught Laboratories Inc [1999] EWCA Civ 1791

Stevens v Kabushiki Kaisha Sony Computer Entertainment (2005) 224 CLR 193

Symes v Saunders [2011] QDC 217

SZSSJ v Minister for Immigration and Border Protection [2014] FCAFC 143

SZTKG v Minister for Immigration and Border Protection [2015] FCA 267

SZTYO v Minister for Immigration and Border Protection (2015) 231 FCR 376

SZULJ v Minister for Immigration and Anor [2015] FCCA 2611

SZUNZ v Minister for Immigration & Anor [2014] FCCA 2256

SZVUM v Minister for Immigration & Anor [2015] FCCA 2263

R *v Adrian Ernest Bayley* [2013] VSC 313

United States Department of Justice v Reporters Committee for Freedom of the Press, 489 US 749

XY v Facebook Ireland Limited [2012] NIQB 96

Norwest Holst Ltd v Department of Trade [1978] Ch 201, 226.

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

Von Hannover v Germany [2004] ECHR 294

Wainwright and Anor v Home Office [2003] 4 All ER 969

Wainwright v Home Office [2002] 3 WLR 405

Wik Peoples v State of Queensland [2004] FCA 1306

Transcript of Proceedings, *David v Abdishou* [2012] HCATrans 253 (October 5 2012)

G *Legislation*

Australian Law Reform Commission Act 1996 (Cth)

Bankruptcy Act 1966 (Cth)

Bankruptcy Regulations 1996 (Cth)

Charter of Fundamental Rights of the European Union 2012/C 326/02

Children's Protection Act 1993 (SA)

Communications Decency Act (1996) US

Competition and Consumer Act 2010 (Cth)

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), as amended by Protocols Nos 11 and 14

County Court Act 1958 (Vic)

Court Suppression and Non-Publication Orders Act 2010 (NSW)

Crimes Act 1914 (Cth)

Data Protection Act 1998 (UK)

E-Government Act of 2002 44 USC § 101 (2002)

Electronic Transactions Act 1999 (Cth)

Family Law Act 1975 (Cth)

Federal Court of Australia Act 1976 (Cth)

Freedom of Information Act 2000 (UK)

Health Records Act 2001 (Vic)

Health Records and Information Privacy Act 2002 (NSW)

Health Records (Privacy and Access) Act 1997 (ACT)

Health Complaints Act 1995 (Tas)

Human Rights Act 2004 (ACT)

Information Act (NT)

Information Privacy Act 2009 (Qld)

Information Privacy Act 2000 (Vic)

Information Privacy Bill 2007 (WA)

International Covenant on Civil and Political Rights, 94th sess, UN Doc CCPR/C/33 (25 June 2009)

Listening Devices Act 1992 (ACT)

Neb. Rev. Stat. § 29-40001.01(09) (2010)

Privacy Act 1988 (Cth)

Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth)

Personal Information Protection Act 2004 (Tas)

Privacy and Personal Information Protection Act 1998 (NSW)

Public Governance, Performance and Accountability Act 2013 (Cth)

Right to Information Act 2009 (Tas)

State Records Act 2000 (WA)

Supreme Court of Queensland Act 1991 (Qld)

Telecommunications Act of 1996I 47 USC 609

Telecommunications (Interception and Access) Act 1979 (Cth)

Universal Declaration of Human Rights, GA Res 217A (111), UN GAOR, 3rd sess, 183rd plen mtg, UN Doc A/810 (10 December 1948)

Witness Protection Act 1995 (NSW)

H *Newspaper/magazine articles*

Bowcott, Owen, 'Superinjunctions: Modern technology out of control, says lord chief justice' *theguardian* (online), 20 May2011 <https://www.theguardian.com/law/2011/may/20/superinjunction-modern-technology-lord-judge>

Fewster, Sean, 'Judges set to overrule court of public opinion', *Advertiser* (Adelaide), 27 October 2014

Giles, Martin, 'Privacy 2.0: Give a little, take a little', *The Economist* (online), 30 January 2010 <http://www.economist.com>

Hasham, Nicole, 'Asylum-seeker victim of government privacy breach fears being murdered by Taliban', *The Sydney Morning Herald* (Sydney), 11 July 2015

Ireland, Judith, 'Refugees could win status over breach', *The Sydney Morning Herald* (Sydney) 20 February 2014, 7

Manning, James, 'Face up to social reality', *The Sydney Morning Herald* (Sydney), 20 June 2012

Moran, Rob, 'Anna Kendrick spent a whole day hilariously live-tweeting her jury duty', *Daily Life* (online), 30 September 2015 <http://www.dailylife.com.au/dl-people/dl-entertainment/anna-kendrick-spent-a-whole-day-hilariously-livetweeting-her-jury-duty-20150929-gjxpqq.html>

Powles, Julia and Enrique Chaparoo, 'How Google determined our right to be forgotten', *The Guardian* (online), 18 February 2015 <http://www.theguardian.com/technology>

Robins, Jon, 'Access to justice is a fine concept. What does it mean in view of cuts to legal aid?' *theguardian* (online), 6 October 2011 < http://www.theguardian.com/law/2011/oct/06/access-to-justice-legal-aid-cuts>

Rosen, Jeffrey, "The Eroded Self' *The New York Times Magazine* (online), 30 April 2000 <http://www.nytimes.com/2000/04/30/magazine/the-eroded-self.html?mcubz=0>

Russell, Mark, 'Isac Ayoul Daing jailed for beating girlfriend Maryanne Sidai to death with kitchen stool' (August 24, 2015) *The Age*

Scheer, David, 'For Your Eyes Only – Europe's New High-Tech Role: Playing Privacy Cop to the World *A1, Wall Street Journal* (New York), 10 October 2003 <https://www.wsj.com/articles/SB106574949477122300>

Schofield, J, 'A Utopia for Thieves' *The Guardian* (online), 29 April 2004 <http://www.theguardian.com/technology/2004/apr/29/viruses.security>

Snow, Deborah and James Manning, 'Modern-day droogs are free to roam' *News Review, The Sydney Morning Herald* (Sydney), 15-16 September 2012

Sprenger, Polly, 'Sun on Privacy: "Get Over It"' *Wired* (online) 26 January 1999 <https://www.wired.com/1999/01/sun-on-privcy-get-over-it>

Steel, Emily and Geoffrey A. Fowler, 'Facebook in Privacy Breach' *The Wall Street Journal* (online), 17 October 2010 <http://online.wsj.com>

Williams, George, 'privacy: the fix should not be left to judges' *The Sydney Morning Herald* (Sydney), 26 March 2013

Economist, 'Special Report: Social networking' *The Economist* (online) 28 January 2010 <http:www.economist.com>

J *Conference Papers*

Allsop, Chief Justice James, 'Values in Law: How They Influence and Shape Rules and the Application of Law' (Paper presented at the Centre for Comparative and Public Law, Faculty of Law, University of Hong Kong, Third Hochelaga Lecture, 20 October 2016)

boyd, danah, and Kate Crawford, 'Six Provocations for Big Data' (Paper presented at Oxford Internet' Institute's "A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society", Oxford, 21 September 2011)

Australasian Institute of Judicial Administration, *Justice Without Barriers: Technology for Greater Access to Justice* (21-22 May, 2015) Brisbane

Banisar, David, 'Catching Up with the Transparency Revolution' (Paper presented at the Justice Wide Open conference, City University, London, 29 February 2012) <https://www.theguardian.com/commentisfree/libertycentral/2012/apr/03/guardian-court-victory-transparency>

Bathurst, Chief Justice T F, 'Social Media: The End of Civilization" Warrane Lecture, the University of New South Wales, Sydney (21 November 2012)

Bathurst, Chief Justice T F, 'Reformulating Reform: Courts and the Public Good' (Paper delivered at the Opening of Law Term Address, 4 February, 2015)

Clarke, Roger, 'What's "Privacy"? (2006) prepared for a Workshop at the Australian Law Reform Commission on 28 July 2006 <http://www.rogerclarke.com>

Givens, Beth, 'Public Records on the Internet: The Privacy Dilemma' (Paper presented at the 12th Annual Conference on Computers, freedom and privacy, San Francisco, 16 – 19 April 2002) <https://www.cfp2002.org/proceedings/proceedings/givens.pdf>.

Griffiths, Justice John, 'Privacy Litigation: Substantive Lessons and Tactical Trends – Smallbone v New South Wales Bar Association' (Paper delivered at 2nd National Information Law Conference, Canberra, 15 November 2012)

Krawitz, Marilyn, 'Challenges of Social Media for Courts & Tribunals' (Issues Paper for the Australasian Institute of Judicial Administration and the Judicial Conference of Australia, Symposium: *Challenges of Social Media for Courts & Tribunals*, Melbourne, 26-27 May)

Kirby, Justice Michael, 'New Frontier – Regulating Technology by Law and "Code"' (Paper at King's College School of Law, London, 8 April 2007)

McLachlin, Chief Justice Beverly, 'Openness and the Rule of Law', (Paper presented at the Annual International Rule of Law Lecture, London, 8 January 2014)

McColl, Justice Ruth, 'An Australian Perspective on Privacy Law Developments' address to the Media Law Resource Centre Conference, London, 30 September 2009

Martin, Chief Justice Wayne, 'Access to Justice: The Media, the Courts and the Public Record' 2009) Paper presented to the Australian Press Council, University, 22 March 2007)

Martin, Chief Justice Wayne, 'Improving Access to Justice: The Role of the Media' (Paper presented to the School of Media, Culture and Creative Arts, Curtin University, 15 October 2009)

Martin, Chief Justice Wayne, 'Improving Access to Justice: The Role of the Media' (Paper presented to the School of Media, Culture and Creative Arts, Curtin University, 15 October 2009)

Martin, Chief Justice Wayne, 'Access to Justice' (Paper presented Inaugural Lecture, Notre Dame University, Eminent Speakers' Series, Fremantle, Wednesday 26 February 2014)

Neuberger, Lord, 'Open Justice Unbound?' (Speech delivered at Judicial Studies Board Annual Lecture, 16 March 2011)

Neuberger, Lord, 'Justice in a Time of Economic Crisis and in the Age of the Internet' (Paper presented for the High Sheriff's Lecture, Leeds, 13 October 2011)

Neuberger, Lord, 'Privacy in the 21st Century' (Paper presented to the UK Association of Jewish Lawyers and Jurists' Lecture, London, 28 November 2012)

Neuberger, Lord, 'Justice in an Age of Austerity' (Paper presented for JUSTICE, Tom Sargant Memorial Lecture 2013, London, 15 October 2013)

Neuberger, Lord, 'The Third and Fourth Estates: Judges, Journalists and Open Justice' (Paper presented at the Hong Kong Foreign Correspondents Conference, 26 August 2014)

Neuberger, Lord, 'Is nothing secret? Confidentiality, Privacy, Freedom of Information and Whistleblowing in the Internet Age' (Speech presented at the Singapore Academy of Law Annual Lecture 2015, Singapore, 21 September 2015)

Perry, Justice Melissa, 'iDecide: the legal implications of automated decision-making' (Paper presented at the Cambridge Centre for Public Law Conference 2014, *Process and Substance in Public Law*, University of Cambridge, Cambridge, 15-16 September, 2014)

Raper, Elizabeth, 'PokeMe: Rights and Responsibilities of Employers and Employees in the Age of Twitter, Facebook, YouTube and MySpace' (Paper presented to the NSW Young Lawyers Seminar, 20 June 2009)

Rares, Justice Steven D, "How the implied Constitutional Freedom of Communication on Government and Political Matter May Require the Development of the Principles of Open Justice' Judicial Conference of Australia Colloquium, 2007, Sydney

Sackville, Justice Ronald, 'From Access to Justice to Managing Justice: The Transformation of the Judicial Role' (Paper presented to the Australian Institute of Judicial Administration Annual Conference *Access to Justice – The Way Forward*, 12-14 July 2002)

Sackville, Ronald, 'Some Thoughts on Access to Justice' (Paper presented at the First Annual Conference on The Primary Functions of Government Courts, Victoria University of Wellington, New Zealand, 28-29 November 2003) *Federal Judicial Scholarship* <http://www.austlii.edu.au>

Sackville, Justice Ronald, 'From Access to Justice to Managing Justice: The Transformation of the Judicial Role' (Paper presented to the Australian Institute of Judicial Administration Annual Conference, Brisbane, 12-14 July 2002)

Shirvington, Virginia, 'Avoiding a Breach of the Professional Conduct and Practice Rules' (Paper presented to the Law Society of New South Wales, 12 March 2001)

Spigelman, Chief Justice J, 'Access to Justice and Access to Lawyers' Paper presented at the 35th Australian Legal Convention, Sydney, 24 March 2007)

Spigelman, J., 'Seen to be Done: The Principle of Open Justice' (Keynote address presented at 31st Australian Legal Convention, Canberra, 1999)

Warren, Marilyn, Chief Justice, 'Embracing Technology: The Way Forward for the Courts' (Papter presented at the 23rd Biennial Conference of District and County Court Judges, Australia and New Zealand, Melbourne, 19 April 2015)

Warren, Marilyn, Chief Justice, 'Courts and our democracy – Just another government agency? Public misapprehension of the role of the Courts' (Paper presented at the Public Forum, Centre for Public Policy, University of Melbourne, Melbourne, 1 May 2012)

Wasserman, Anthony I, 'Software Engineering issues for Mobile Application Development' (Paper presented at the Workshop on Mobile Software Engineering, Santa Clara, 28 October 2010) <http://www.mobileworkshop.org>

Zorza, Richard, 'Review of the Status and Potential of Access to Justice Technology in the United States of America' (Paper presented at the International Legal Aid Group meeting, June 2013) <http://www.zorza.net>

K *Unpublished works/theses*

Bevan, Kitrina Lindsay, *Clerks and Scriveners: Legal Literacy and Access to Justice in Late Medieval England* (2013) thesis submitted for the degree of Doctor of Philosophy in Law, University of Exeter

Klang, Mathias, *Disruptive Technology: Effects of Technology Regulation on Democracy*, (2006) thesis submitted for the degree of Doctor of Philosophy in Law, Göteborg University <http://hdl.handle.net/2077/9910>

L Other

Australian Government, 'A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy', Issues Paper (23 September 2011) <https://www.ag.gov.au/Consultations/Pages/Righttosueforseriousinvasionofpersonalprivacyissuespaper.aspx>

Barlow, John Perry, 'A Declaration of the Independence of Cyberspace' <https://www.eff.org/cyberspace-independence>

Bruns, Axel, 'Ad hoc innovation by users of social networks : the case of Twitter', In Soziale Innovation – (2012) Centre for Social Innovation , Zentrum für (Ed.) *ZSI Discussion Paper*, Zentrum für Soziale Innovation – Centre for Social Innovation , Tech Gate Vienna, Donau-City-Straße 1, Vienna Austria, 1

David, Ian, 'Talis, Web 2.0 and All That' *Internet Alchemy* blog (4 July 2005) <http://iandavid.com/2005/07/talis-web-2-0-and-all-that/>

Director of Public Prosecutions, 'Interim guidelines on prosecuting cases involving communication sent via social media' (19 December 2012) <http://cps.gsi.gov.uk>

European Commission, 'EDPS welcomes a "huge step forward for data protection in Europe", but regrets inadequate rules for the police and justice area' (Press Release, EDPS/12/2, 25 January 2012) <http://europa.eu/rapid/search.htm>.

Floridi, Luciano, 'Right to be Forgotten: A Diary of the Google Advisory Council Tour' (2014) <http://www.philosophyofinformation.net/right-to-be-forgotten-a-diary-of-the-google-advisory-council-tour/>

Gurría, Angel, 'Closing remarks by Angel Gurría, OECD Ministerial Meeting on the Future of the Internet Economy' (Speech delivered at the OECD Ministerial Meeting on the Future of the Internet Economy, 18 June 2008) <http://www.oecd.org/korea/closingremarksbyangelgurriaoecdministerialmeetingonthefutureoftheinterneteconomy.htm>

Judicial Press Office, Judiciary of England and Wales, 'Committee Reports Findings on "Super-Injunctions" (Media Release, 20 May 2011) <http://www.judiciary.gov.uk/media/media-releases>

Sensis, *Aging face of social media* (Sensis, 29 May 2014) <http://www.sensis.com.au/about/news/aging-face-of-social-media>

Strickland, Jonathan, 'How Web.20 Works' (20 January 2016) HowStuffWorks <http://computer.howstufworks.com/web-2.0htm>

Thierer, Adam, 'Public Interest Comment on Federal Trade Commission Report, *Protecting Consumer Privacy in an Era of Rapid Change*' (2011) <https://www.ftc.gov/sites/.../public_comments/...ftc-staff-report.../00320-57670.pdf>

Waters, Nigel and Graham Greenleaf, 'A critique of Australia's proposed *Privacy Amendment (Enhancing Privacy Protection) Bill 2012*' (Research Paper No 2012-35, UNSW Law) <https://papers.ssrn.com>

Washington State Supreme Court, *Access to Justice Principles* (3 December 2004) <http://www.atjweb.org>

On Mon, Jul 28, 2014 at 2:35 PM, Faculty of Arts Research Office <artsro@mq.edu.au> wrote:

Ethics Application Ref: (5201400688) - Final Approval

Dear Dr Selvadurai,

Re: ('The Digital Pathway to Justice - Access or Privacy? - detailed study of eCourtroom in the Federal Court of Australia and the Federal Circuit Court of Australia')

Thank you for your recent correspondence. Your response has addressed the issues raised by the Faculty of Arts Human Research Ethics Committee. Approval of the above application has been granted, effective (28/07/2014). This email constitutes ethical approval only.

If you intend to conduct research out of Australia you may require extra insurance and/or local ethics approval. Please contact Maggie Feng, Tax and Insurance Officer from OFS Business Services, on x1683 to advise further.

This research meets the requirements of the National Statement on Ethical Conduct in Human Research (2007). The National Statement is available at the following web site:
http://www.nhmrc.gov.au/_files_nhmrc/publications/attachments/e72.pdf.

The following personnel are authorised to conduct this research:

Dr Niloufer Selvadurai
Mrs Jennifer Kaye Farrell
NB. STUDENTS: IT IS YOUR RESPONSIBILITY TO KEEP A COPY OF THIS APPROVAL EMAIL TO SUBMIT WITH YOUR THESIS.

Please note the following standard requirements of approval:

1. The approval of this project is conditional upon your continuing compliance with the National Statement on Ethical Conduct in Human Research (2007).

2. Approval will be for a period of five (5) years subject to the provision of annual reports.

Progress Report 1 Due: 28th July 2015
Progress Report 2 Due: 28th July 2016
Progress Report 3 Due: 28th July 2017
Progress Report 4 Due: 28th July 2018
Final Report Due: 28th July 2019

NB: If you complete the work earlier than you had planned you must submit a Final Report as soon as the work is completed. If the project has been discontinued or not commenced for any reason, you are also required to submit a Final Report for the project.

Progress reports and Final Reports are available at the following website:
http://www.research.mq.edu.au/for/researchers/how_to_obtain_ethics_approval/human_research_ethics/forms

3. If the project has run for more than five (5) years you cannot renew approval for the project. You will need to complete and submit a Final Report and submit a new application for the project. (The five year limit on renewal of approvals allows the Committee to fully re-review research in an environment where legislation, guidelines and requirements are continually changing, for example, new child protection and privacy laws).

4. All amendments to the project must be reviewed and approved by the Committee before implementation. Please complete and submit a Request for Amendment Form available at the following website:
http://www.research.mq.edu.au/for/researchers/how_to_obtain_ethics_approval/human_research_ethics/forms

5. Please notify the Committee immediately in the event of any adverse effects on participants or of any unforeseen events that affect the continued ethical acceptability of the project.

6. At all times you are responsible for the ethical conduct of your research in accordance with the guidelines established by the University. This information is available at the following websites: http://www.mq.edu.au/policy/
http://www.research.mq.edu.au/for/researchers/how_to_obtain_ethics_approval/human_research_ethics/policy
If you will be applying for or have applied for internal or external funding for the above project it is your responsibility to provide the Macquarie University's Research Grants Management Assistant with a copy of this email as soon as possible. Internal and External funding agencies will not be informed that you have approval for your project and funds will not be released until the Research Grants Management Assistant has received a copy of this email.

If you need to provide a hard copy letter of approval to an external organisation as evidence that you have approval, please do not hesitate to contact the Faculty of Arts Research Office at ArtsRO@mq.edu.au
Please retain a copy of this email as this is your official notification of ethics approval.
Yours sincerely

Dr Mianna Lotz
Chair, Faculty of Arts Human Research Ethics Committee
Level 7, W6A Building
Macquarie University
Balaclava Rd
NSW 2109 Australia
Mianna.Lotz@mq.edu.au

Macquarie Law School
Faculty of Arts
MACQUARIE UNIVERSITY NSW 2109

Phone: +61 (0)2 9850 7925
Fax: +61 (0)2 9850 7686

Email: niloufer.selvadurai@ mq.edu.au

Niloufer Selvadurai:

Associate Professor, Macquarie Law School

Deputy District Registrar, Federal Court

A Registrar, Federal Circuit Court

Federal Court of Australia

Level 17, Law Courts Building

Queens Square

Sydney NSW 2000

Dear

Participant Information and Consent Form

Name of Project: A detailed examination of the use of eCourtroom in the Federal Court and the Federal Circuit Court of Australia. This is part of the dissertation: *The Digital Pathway to Justice – Access or Privacy?*

You are invited to participate in a study of eCourtroom. The purpose of the study is to examine the use of electronic litigation in a virtual courtroom. This project will examine the digital pathway, particularly the access provided and the privacy issues involved.

The study is being conducted by *Associate Professor Niloufer Selvadurai as Chief Investigator and Jennifer Farrell as Co-Investigator.* The research is being conducted to meet the requirements of Doctor of Philosophy in Law under the supervision of Associate Professor Niloufer Selvadurai of the Department of Macquarie Law School, Ph (w) (02) 9850 7925, Email: niloufer.selvadurai@mq.edu.au

If you decide to participate, you will be asked to answer five questions about your experience using eCourtroom. The questions will be open-ended. Each question should take approximately 5 – 10 minutes to answer. The response required should only be about two to three short paragraphs and the total written response no more than two pages.

Any information or personal details gathered in the course of the study are confidential, except as required by law. No individual will be identified in any publication of the results. Access to the data will be provided to the Chief Investigator and Co-Investigator only. A summary of the results of the data can be made available to you on emailing your request to the Co-Investigator. Participants' quotes may be used but the participants will be de-identified.

Participation in this study is entirely voluntary: you are not obliged to participate and if you decide to participate, you are free to withdraw at any time without having to give a reason and without consequence.

I, *(participant's name)* have read and understand the information above and any questions I have asked have been answered to my satisfaction. I agree to participate in this research, knowing that I can withdraw from further participation in the research at any time without consequence. I have been given a copy of this form to keep.

Participant's Name:_____

(Block letters)

Participant's Signature:_____ Date:_____

Investigator's Name:_____

(Block letters)

Investigator's Signature: _____ ___ Date:_____

The ethical aspects of this study have been approved by the Macquarie University Human Research Ethics Committee. If you have any complaints or reservations about any ethical aspect of your participation in this research, you may contact the Committee through the Director, Research Ethics (telephone (02) 9850 7854; email ethics@mq.edu.au). Any complaint you make will be treated in confidence and investigated, and you will be informed of the outcome.

(INVESTIGATOR'S [OR PARTICIPANT'S] COPY)

Appendix C: Content coding of responses to questionnaire

Question Number	Item/Phrase	Main Category
1 **Experience in hearing matters**	**'ex parte 'chambers' application'**	*Procedure*
	'text focussed'	*Communication*
	'substituted service applications in bankruptcy and examinations in bankruptcy and insolvency'	*Procedure*
	'used mainly in the Federal Circuit Court'	*Procedure*
	'save costs'	*Efficiency*
	'greater flexibility in time'	*Efficiency*
	avoid the necessity of 'face to face hearing'	*Efficiency*
	'very useful tool'	*Efficiency*
	'efficient'	*Efficiency*
	'access e-court at any time'	*Efficiency*
	'easy to use'	*Efficiency*
	'Initially … communications overly informal or personal'	*[disadvantages]* *Efficiency*
		Technology
		Procedure
		Communications
2 **Advantages**	**No physical attendance in court**	*Efficiency*
	Advantage for the applicant rather than the court	*Efficiency*
	Written communication – greater clarity	*Communication*
	Greater consistency in application of the law	*Administration of Justice*
	Matters can be listed sooner	*Efficiency*
	Better use of time, especially if the orders are long and complex – not need physical court time	*Efficiency*
	No waiting time	

	Any time of the day	*Efficiency*
	Flexible	*Efficiency*
	Efficiency	*Efficiency*
	Cost savings in use of court facilities	
	More convenient	*Efficiency*
	Orders made faster	
	Embraces use of technology in a court environment	*Technology*
	Regular practitioners who file – familiar with procedure	*Representation*
	Important for a national court – can be anywhere	*Efficiency*
	Savings can be passed on to clients	
	"not time sensitive"	*Efficiency*
	Quicker when familiar with software	*Technology*
	Save cost of personal attendance	*Efficiency*
	Detailed written records	*Communication*
3 Disadvantages		
	Substantive submissions	*Procedure*
	Self-represented	*Representation*
	Complex matters	*Procedure*
	Time delay for response	*Efficiency*
	Cumbersome	*Efficiency*
	Less experienced practitioners – paralegals	*Practitioners*
	No contradictor	*Administration of Justice*
	Information and discursive	*Communication*
	Can be longer to respond where application refused	*Efficiency*
	Computer skills	*Technology*
	Program issues	*Technology*
	Factual disputes	*Procedure*

	'more efficient in normal court room'	
	'hearing can take considerably longer'	
	'not necessarily the best medium'	
	'transition' to use of eCourtroom smooth	
4 **Public access, privacy**	**eCourtroom "mirrors open court"**	*Administration of Justice*
	private data - sensitive	*Privacy*
	affidavits in support	*Privacy*
	some restriction to final order – respondent could continue to avoid service	*Regulation*
	transcript useful for Registrars	*Procedure*
	no live public transcript	*Privacy*
	redact evidence prior to third party access	*Privacy*
5 **Other uses** **skype**	**Extend the life of petition**	*Procedure*
	Security for costs	*Procedure*
	Extension of time applications	
	Call-overs	
	Directions	
	Summons for examination	*Procedure*
	S596A corporations examinations	
	Skype may allow "usual dynamics of human communication"	*Communication*
	Not designed for contested applications	*Procedure*
	Time consuming	*Efficiency*
	Difficult to use in other than ex parte applications	*Procedure*
	Useful matters being decided on submissions	*Efficiency*
	Short service applications	*Procedure*
	Unrealistic to expect practitioners to have technology	*Technology*
	Useful for procedural matters	*Procedure*
	Not so useful where 'active advocacy' required.	*Administration of Justice*

	Probably not different if skype available – useful for procedural matters	*Procedure*
	Lodgement of bills of costs, appeal index conferences, consent adjournment application; setting down mediations – procedural matters	*Procedure*
	Skype could alleviate some of difficulties of 'written response'?	*Technology*
	Mediations instead of by phone	
	Possible saving	*Procedure*
	Maybe problem with informality	*Efficiency*
	eCourtroom – limited application; 'value the right to address the decision maker in Court' – 'not erode lightly'	*Communication*
	skype not sufficiently reliable technology; already use video link	*Administration of Justice*
	need oral evidence in controlled court room environment	*Technology* *Administration of justice*