to proactively identifying and removing child abuse material from the web, as evidenced by our work on PhotoDNA which is a technology used on Microsoft and other social networking to automatically identify child abuse material.

Identified Contact Person:
The local contact person is James Kavanagh, Chief Security Advisor for Microsoft Australia.

Education and Awareness Raising & Collaboration with Government:
Microsoft has extensive information available online, usually displayed in the context of the particular user's interaction. Microsoft participates with the Department's activities such as Cyber Security Awareness Week to raise awareness of cyber safety and security more broadly.

Specifically in relation to social networking, Microsoft in partnership with the Australian Federal Police and nineMSN launched the highly successful ThinkUKnow program to help parents better guide their children in having safe interactions online.

Continued Innovation:
Microsoft is deeply committed to bringing innovations that promote a safer online environment. This is evidenced by commitment to programs like PhotoDNA and the Child Exploitation Tracking System (CETS), and by fundamental innovations within our technology platform such as SmartScreen in Internet Explorer.

Transparency:
Through existing engagement mechanisms with the Australian Government and direct engagement through our local Chief Security Advisor, this level of engagement and transparency is already in place.

3. Other actions taken on implementation of these arrangements

Microsoft's existing policies and practices are sufficient to give effect to these arrangements.

Cooperative Arrangements for Complaints Handling on Social Networking Sites

Yahoo!7

In the interests of transparency, providers supporting the Cooperative Arrangements for Complaints Handling on Social Networking Sites agree to provide information on how they give effect to the Principles in relation to social networking services they offer, using this form.

1. About the Social Networking Service

YAHOO!7

Yahoo!7 (yahoo7.com.au) is one of the most comprehensive and engaging online destinations for Australian consumers and advertisers. Formed as a 50-50 partnership between the Seven West Media Group and Yahoo! Inc. Yahoo!7 brings together the successful Australian internet business, Yahoo! Australia & NZ, and the online assets and television and magazine content of the Seven Network, one of Australia's leading media companies. The company also combines the strengths of Yahoo! search and communications capabilities and its global internet network, with Seven's rich media and entertainment content and marketing capabilities. Yahoo!7 has a significant local presence employing over 360 people based across our businesses in Australia and New Zealand.

Yahoo!7 offers a range of 'social networking' services through our products Flickr (photo sharing), Yahoo!7 Video (commercial and user generated video sharing), Yahoo!7 Answers (knowledge sharing), Spreets (group buying) and Yahoo!7 mail and instant messenger.

As the Internet pioneer with over 17 years in this domain, Yahoo! has dealt with safety related issues in different parts of the world and has acquired experiential wisdom and valuable expertise on how to remain smart, safe and responsible online.

Safety, transparency and responsiveness are top line priorities for Yahoo!7. We innovate with these goals in mind and see advanced yet accessible privacy and safety features as not only a competitive advantage but an absolute necessity in the provision of social networking services.

2. How will the provider give effect to the complaints handling aspect of the Cooperative Arrangement?

Policies for Acceptable Use: Anyone can access the Yaoo!7 website or create a Yahoo!7 account. By creating an account all visitors are subject to the Yahoo!7 Terms of Service ("TOS") (http://info.yahoo.com/legal/au/yahoo/utos/en-au/). The TOS include a detailed section on member conduct which clearly explains what is allowed on the Yahoo!7 platform and what is not.

Complaints Mechanisms and Review Process: Yahoo!7 provides tools to assist in reporting inappropriate or harmful behavior such as our "Report Abuse" buttons and the Abuse Help Forms. The Yahoo!7 "Report Abuse" buttons are conspicuously located alongside each item of user generated content and appear at the footer of every Flickr page. A user simply needs to click this button to instantly report the specific piece of content to Yahoo!7 for review and where appropriate removal.

Yahoo!7 builds accessible safety and privacy features into all our social networking products, including privacy preferences, blocking capabilities, flagging and content filters and FAQ safety guides (specific to Y!7 products: http://au.safely.yahoo.com/yahoo-products/ and general online tips: http://au.safely.yahoo.com/faq/). For example the Flickr SafeSearch tool allows users to remove content from a search result that isn't suitable for all ages. This feature is turned on by default for all new accounts.

[See the below section on Education and Awareness Raising for further information.]

Child Abuse Material: Yahoo!7 works closely with Australian law enforcement agencies to provide assistance when Yahoo!'s services are being abused including the establishment of a 24 x 7 compliance function that can immediately respond to law enforcement if we are contacted about a situation that indicates that a child may be in danger or relates to the circulation of child abuse material.

Yahoo!7 provides training to the law enforcement community to increase awareness of how Yahoo! products and services work and how to obtain information from us. Yahoo!7 has created an Australian Law Enforcement Process Guide designed to ensure that law enforcement personnel are familiar with Yahoo!7's policies, procedures, and systems, and clearly understand how to obtain the appropriate investigatory information in child exploitation cases.

Yahoo!7 does not tolerate images of child sexual exploitation on its network, and upon becoming aware of such images, Yahoo!7 removes them from its network and reports such images to the appropriate authorities. Any time Yahoo!7 becomes aware of images of apparent child pornography, those images are removed from our network and referred to Yahoo! Inc. (Yahoo!7's parent company). Yahoo! Inc. in turn reports those images to the U.S. National Center for Missing and Exploited Children as required by US law. NCMEC in turn will refer such reports with an Australian nexus to Australian law enforcement.

Identified Contact Person: Yahoo!7 has an Australia-based contact person who deals with law enforcement and user safety issues and an identified representative on the Government's Consultative Working Group on Cybersafety with whom the Government can have direct dialogue regarding developing issues that may require prompt attention and response.

Education and Awareness Raising: Yahoo! is a longtime industry leader on child safety and has made it a company priority to promote safer and more responsible use of online technology and mobile phones among children and young people globally. Yahoo! is a thought leader in this important space and works collaboratively with its industry peers, child safety groups, and law enforcement to find new ways to protect children online.

Yahoo!7 has a dedicated 'Safely' website at http://au.safely.yahoo.com/ with specific sections targeted to teens and adults providing practical advice and guidance on improving safety online, including: location services, choosing a secure online ID and strong secure passwords, managing children's search queries, mobile safety tips, parental controls, protection of privacy, tips for to help prevent cyberbullying and links to external resources.

The Safely website also includes safety specific information specific to each of Yahoo!7's communications products (such as Mail, Flickr, Messenger) highlighting technical tools and best practices with regard the use of these services.

Yahoo!7's Privacy Centre (http://info.yahoo.com/privacy/au/yahoo/) provides a one stop, easy to understand information resource where account holders can review and adjust their privacy preferences. The Privacy Centre also provides a highly visible one click opt-out button where users can elect not to receive interest-matched advertising while using the Yahoo!7 platform.

Outside of Australia Yahoo! hosts an annual Digital Citizenship Summit in the US bringing together teachers, administrators and support staff with Internet safety experts to facilitate dialogue, collaboration and share best-practices around online safety issues. Themes have covered bullying prevention, digital reputation and building a culture of safety and respect.

Collaboration with Government on Education and Awareness Raising Initiatives: In Australia, Yahoo!7 has been an active participant in Safer Internet Day over the past two years, promoting the ACMA Cybersmart website and the CyberSafety Help Button within the Yahoo!7 Mail and Messenger products. We are also participants in Privacy Awareness Week, contributors to the Easy Guide to Socialising Online and a supporter of the annual National CyberSecurity Awareness Week.

Continued Innovation: Yahoo! supports and partners with non-profit organisations all over the world who, amongst other things, undertake research on safety issues including:

- ikeepsafe.org
- Family Online Safety Institute (FOSI)
- National Centre for Missing & Exploited Children (NCMEC)
- StopCyberbullying.org
- ChildNet
- ConnectSafely

Yahoo! has implemented technology and policies to help identify apparent child pornography violations on our global network. These include using a combination of filters, algorithms, and human review, as well as user reports of abuse.

Yahoo! has partnered with the US based National Centre for Missing and Exploited Children and U.K. based Internet Watch Foundation in an effort to reduce the proliferation of child pornography by removing known apparent child pornography URLs from Yahoo! search index results and responding to any apparent child pornography violations on our network.

Yahoo! has enabled a "SafeSearch" feature within Yahoo!7 Search to prevent display of adult content in search queries made by that user's Yahoo! account (turned on by default). Parents can lock SafeSearch on to prevent children from turning it off. On Yahoo!'s mobile service "onesearch", all users default to SafeSearch mode and children registered as under 17 cannot turn the function off.

Yahoo!7 also offers account holders the ability to create a unique sign-in seal to protect from phishing sites. A sign-in seal is a secret message or photo hat Yahoo! will display on a genuine Yahoo!7 website when you log in. If the seal isn't displayed then a user will know they may have landed on a phising page.

3. Other action taken on implementation of these arrangements

Yahoo!7 makes safety a company priority by supporting efforts to educate children, parents, adults, and communities about safe online experiences. Yahoo!7 will continue to take a multi-faceted approach in promoting a safer online experience including encouraging parents to use Yahoo! Safely to access relevant, up-to-date strategies and tools to help foster safer online experiences.

Ellery, Jacqueline

From: s47F
Sent: Thursday, 11 October 2012 10:50 AM
To: Ellery, Jacqueline
Cc:
Subject: s47F RE: Social Media and the Law [SEC=UNCLASSIFIED]

UNCLASSIFIED

Hi Jackie

This is something my branch has been dealing with (along with our Justice Policy and Administrative Law Branch). AGD will have an involvement in the Victorian Working Group.

Branch Ananijevski is our contact (ph. 6141 3108) and he will get in touch with you.

Regards,
s47F

s47F
Assistant Secretary
Criminal Law and Law Enforcement Branch
Attorney-General's Department
Robert Garran Offices | National Circuit | Barton ACT 2600
p 6141 2800
s47F

From: s47F
Sent: Thursday, 11 October 2012 9:35 am
To: s47F
Subject: FW: Social Media and the Law [SEC=UNCLASSIFIED]

UNCLASSIFIED

Hi s47F

Is this something someone in your branch can assist with?

Thanks,
s47F

s47F
Senior Legal Officer – Crime Prevention
Border Management and Crime Prevention Branch
Criminal Justice Division
Attorney-General's Department

s47F
s47F
4 National Circuit

BARTON ACT 2600

From: Ellery, Jacqueline [mailto:Jacqueline.Ellery@afp.gov.au]
Sent: Wednesday, 10 October 2012 11:02 am
To: s47F
Subject: Social Media and the Law [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good morning Fiona,

I'm a relatively new kid on the block in Elsa Sengstock's team and she's asked me to touch base with you about the emerging issues associated with the social media and more particularly the impact it may have on criminal trials. We are currently keeping a watch on things, but wondered whether AGD have much interest or involvement at this point?

I note that the SCLJ issued a Communique this week stating the Ministers agreed that the issue be further considered by a working group of the SCLJ being chaired by Victoria to provide recommendations following consultation with various organisations/authorities. Do you know if AGD will have involvement in this process?

I would be happy to have a chat with you about this topic and, from a law enforcement perspective, would appreciate any updates/advice you might have to date. Let me know when it's convenient and perhaps we can touch base.

Kind regards
Jackie

AFP
AUSTRALIAN FEDERAL POLICE

JACQUELINE ELLERY
LEGISLATION PROGRAM
POLICY & GOVERNANCE
Tel +61(0) 2 61313788 Ext 143788 Fax +61(0) 2 61326082
www.afp.gov.au

UNCLASSIFIED

****

WARNING

****

Ellery, Jacqueline

From: s47F
Sent: Thursday, 11 October 2012 9:40 AM
To: Ellery, Jacqueline
Subject: RE: Social Media and the Law [SEC=UNCLASSIFIED]

UNCLASSIFIED

Hi Jackie,

Sorry for not replying to your email yesterday – I was off sick with a cold. This isn't something our branch can help with so I have forwarded your email tc s47F the head of the Criminal Law and Law Enforcement Branch in our Division, to ask whether there is someone there who would have some input.

Kind regards,

s47F

s47F
Senior Legal Officer – Crime Prevention
Border Management and Crime Prevention Branch
Criminal Justice Division
Attorney-General's Department

s47F
s47F
4 National Circuit
BARTON ACT 2600

From: Ellery, Jacqueline [mailto:Jacqueline.Ellery@afp.gov.au]
Sent: Wednesday, 10 October 2012 11:02 am
To: s47F
Subject: Social Media and the Law [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good morning s47F

I'm a relatively new kid on the block in Elsa Sengstock's team and she's asked me to touch base with you about the emerging issues associated with the social media and more particularly the impact it may have on criminal trials. We are currently keeping a watch on things, but wondered whether AGD have much interest or involvement at this point?

I note that the SCLJ issued a Communique this week stating the Ministers agreed that the issue be further considered by a working group of the SCLJ being chaired by Victoria to provide recommendations following consultation with various organisations/authorities. Do you know if AGD will have involvement in this process?

I would be happy to have a chat with you about this topic and, from a law enforcement perspective, would appreciate any updates/advice you might have to date. Let me know when it's convenient and perhaps we can touch base.

Kind regards
Jackie

JACQUELINE ELLERY
LEGISLATION PROGRAM
POLICY & GOVERNANCE
Tel +61(0) 2 61313788 Ext 143788 Fax +61(0) 2 61326082
www.afp.gov.au

UNCLASSIFIED

Ellery, Jacqueline

From: Ellery, Jacqueline
Sent: Wednesday, 10 October 2012 11:02 AM
To: s47F
Subject: Social Media and the Law [SEC=UNCLASSIFIED]

UNCLASSIFIED

Good morning Fiona,

I'm a relatively new kid on the block in Elsa Sengstock's team and she's asked me to touch base with you about the emerging issues associated with the social media and more particularly the impact it may have on criminal trials. We are currently keeping a watch on things, but wondered whether AGD have much interest or involvement at this point?

I note that the SCLJ issued a Communique this week stating the Ministers agreed that the issue be further considered by a working group of the SCLJ being chaired by Victoria to provide recommendations following consultation with various organisations/authorities. Do you know if AGD will have involvement in this process?

I would be happy to have a chat with you about this topic and, from a law enforcement perspective, would appreciate any updates/advice you might have to date. Let me know when it's convenient and perhaps we can touch base.

Kind regards
Jackie

AFP
AUSTRALIAN FEDERAL POLICE

JACQUELINE ELLERY
LEGISLATION PROGRAM
POLICY & GOVERNANCE
Tel +61(0) 2 61313788 Ext 143788 Fax +61(0) 2 61326082
www.afp.gov.au

UNCLASSIFIED

Australian Government

Issues Paper

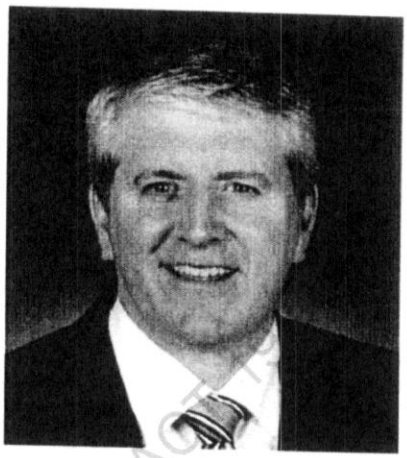
A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy

Commonwealth of Australia
Department of the Prime Minister and Cabinet

September 2011

ISBN 978-1-921739-51-4

Foreword



Every day, many of us take actions to protect our privacy and that of our families, almost without thinking about it. We might close the curtains in our homes at night; ensure no one can see our PIN when we're at the ATM; or leave a meeting to take a personal phone call. Thankfully, simple actions are usually enough and serious invasions of privacy are infrequent.

Rapid advances in technology have changed the way we work, bank and shop, the way people engage with government, and the way we relate to friends, family and people we've never even met. New technology provides new opportunities, but it also provides new challenges – one of which is whether the laws relating to privacy have kept pace with these changes.

Smart phones allow us to take and instantly share photographs, without the knowledge or consent of the subject. A private email can be forwarded to thousands of addresses around the world, and footage posted on a video sharing website can go viral. Email and social networking sites can be hacked and personal details can be mined. Cloud computing offers great potential for more effective and efficient use of technology but its security must be assured.

We have seen recently, both in Australia and overseas, a number of high profile privacy breaches that have arisen, in part, because of the development of new and emerging technological capabilities.

In May 2008, the Australian Law Reform Commission (ARLC) concluded a 28-month inquiry into the effectiveness of the *Privacy Act 1988* and related laws as a framework for the protection of privacy in Australia. In its report, the ALRC made 295 recommendations for reform in a range of areas, including telecommunications, credit reporting information, health records, and privacy protection generally. The Government has responded to 197 of these recommendations.

One of the ALRC's recommendations was that the most serious invasions of privacy could best be addressed through the introduction of a statutory cause of action for privacy. The Victorian and New South Wales Law Reform Commissions have also recommended a statutory cause of action for privacy.

In responding to the ALRC recommendation, the threshold question that must be asked is whether the introduction of a statutory cause of action for privacy is warranted. This is a particularly important question in light of a cause of action for privacy developing case-by-case in the Australian courts. If there is to be a statutory cause of action, how do we make sure it gets the balance right between the public interest in the right to privacy and other important public

interests including freedom of expression? We cannot simply consider whether action is desirable without also considering how best to do it.

The Australian Government has prepared this Issues Paper for public consideration of these important questions. I encourage everyone with an interest to visit www.dpmc.gov.au/privacy/causeofaction/ to submit his or her views on this important debate.

The Hon Brendan O'Connor MP

Minister for Privacy and Freedom of Information

Contents

Request for comments

The Commonwealth Government has developed this issues paper, *A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy*, to inform its response to the Australian Law Reform Commission's recommendations to introduce a statutory cause of action for serious invasions of privacy.

This paper invites comment upon whether Australia should introduce a statutory cause of action for privacy and, if so, what elements a statutory cause of action might include. It draws on the analysis of the Australian, Victorian and New South Wales Law Reform Commissions, and considers the policy context and current legal positions in Australia and comparable jurisdictions.

Submissions may address the particular questions contained in the paper, comment upon the proposed reform as a whole or upon any other relevant issue.

How to provide us with your comments and ideas

Responses are requested **by Friday, 4 November 2011**, though earlier responses are encouraged. Responses submitted in the form of an attachment to an email are preferred.

Responses may be submitted:

By email: privacycauseofaction@pmc.gov.au

By post: Privacy and FOI Policy Branch
Department of the Prime Minister and Cabinet
1 National Circuit
BARTON ACT 2600

Phone: 02 6271 5111
Fax: 02 6271 5542

Publication of Submissions

It will be assumed that submissions are not confidential and may be made publicly available on the website of the Department (http://www.dpmc.gov.au/privacy/causeofaction/).

If you would like your submission, or any part of it, to be treated as confidential, please indicate this clearly on the submission. A request made under the *Freedom of Information Act 1982* (Cth) for a submission marked confidential to be made available will be determined in accordance with that Act.

Introduction

Community concern about the right to and protection of privacy is growing as new technologies change the way we interact with business, government, and each other.

Australians are increasingly connected to the internet at home and work. Digital technologies are readily affordable and available. Online activity is growing and ways of communicating are more diverse. Recording devices in phones are becoming standard. These changes have significant advantages for Australian society, but they also pose commensurate risks to our privacy.

Images, sounds and other information can easily be recorded, and just as easily can be uploaded to the internet, or distributed via email and instant messaging – sometimes without a person's consent or without their knowledge.

Social networking platforms allow extensive online networks to be created and maintained, for links and associations to be made, and for images and information to be widely shared. Once on the web it becomes increasingly difficult for an individual to control.

Privacy may be protected through a range of regulatory, administrative, educational, and legal mechanisms. In Australia, the Commonwealth *Privacy Act 1988*[1], along with privacy and personal information legislation in most States and Territories, seeks to protect the personal and sensitive information of individuals, primarily by requiring that such information be collected and handled appropriately. Laws relating to defamation, telecommunications, breach of confidence and trespass, amongst other things, also offer protection for aspects of the private lives of those resident in Australia.

In its 2008 Report, *For Your Information: Australian Privacy Law and Practice*, the Australian Law Reform Commission (**ALRC**) considered the range of privacy protections available in Australia and made a number of recommendations. As part of that report, the ALRC recommended that federal legislation should provide for a statutory cause of action (a right to sue created by law) for serious invasions of the privacy of natural persons.[2] The New South Wales[3] and Victorian[4] Law Reform Commissions have also recommended similar causes of action.

---

[1] The *Privacy Act 1988* (Cth), as amended, is available at <www.comlaw.gov.au/Series/C2004A03712>.

[2] Australian Law Reform Commission, *Report 108 – For Your Information: Australian Privacy Law and Practice* (2008), ch 74 and recs 74–1 to 74–7 (**ALRC Report**), available at <www.alrc.gov.au/publications/report-108>.

[3] New South Wales Law Reform Commission, *Report 120: Invasion of Privacy* (2009) (**NSWLRC Report**) available at <www.lawlink.nsw.gov.au/lawlink/lrc/ll_lrc.nsf/vwFiles/R120.pdf/$file/R120.pdf>.

[4] Victorian Law Reform Commission, *Surveillance in Public Places: Final Report 18* (2010), ch 7 (**VLRC Report**) available at <www.lawreform.vic.gov.au/wps/wcm/connect/justlib/Law+Reform/Home/Completed+Projects/Surveillance+in+Public+Places/>.

In 2009, the Government responded to 197 of 295 recommendations of the ALRC Report. At that time, the Government announced that it would consider the ALRC's remaining recommendations, including a statutory cause of action, following work on the first stage reforms.[5] Those first stage reforms are progressing: exposure draft legislation relating to new Australian Privacy Principles (APPs) and credit reporting has been referred to the Senate Finance and Public Administration Committee in June 2010 and January 2011 respectively. That Committee has now reported on the first of those references.

This paper asks whether Australia should introduce a statutory cause of action for privacy and, if so, what elements a statutory cause of action might include. This paper draws on the reports and analysis of the ALRC[6], the New South Wales Law Reform Commission (**NSWLRC**)[7] and the Victorian Law Reform Commission (**VLRC**)[8], and considers the current legal position in other comparable jurisdictions. It begins with a review of some of the present context within which these privacy matters may be considered.

---

[5] See *Australian Government First Stage Response to Australian Law Reform Commission Report 108: For Your Information: Australian Privacy Law and Practice* at 6:

> We will start with reforming the foundations. Once these reforms have progressed, the Government will turn to considering the remaining recommendations of the ALRC. These recommendations include sensitive and complex questions around the removal of exemptions and data breach notices. To strike the right balance, reforms in these areas will require extensive consultation and input.

[6] The ALRC recommendations are reproduced in Appendix A at page 54 below.

[7] The draft bill recommended by the NSWLRC is reproduced in Appendix B at page 56 below.

[8] The VLRC recommendations are reproduced in Appendix C at page 64 below.

The current privacy context

In 1937, the High Court was asked to decide whether Australians had a right to privacy. In finding that no such right existed under Australian common law, Chief Justice Latham stated:

> Any person is entitled to look over the plaintiff's fence and to see what goes on in the plaintiff's land. If the plaintiff desires to prevent this, the plaintiff can erect a higher fence.[9]

Today, the privacy context is drastically different from that of 1937, and indeed the whole of the 20th century. Developments in technology have meant that it is more difficult for individuals to take steps to protect their own privacy by the mere erection of a higher fence.

Some of the key technological developments that have changed the context for the protection of privacy in Australian society include:

- greater access to technology;
- increased connection to the internet;
- faster internet speeds;
- growth in the level of online activity; and
- the expansion of online social networks.

Technology is becoming affordable and accessible. Economies of scale, improvements in productivity, more efficient use of raw materials, and competition mean that a wide range of technology is cheaper for consumers and therefore more attainable. In the decade to 2008-09 household access to a computer increased from 44% to 78%.[10] Improvements in storage technologies and hardware mean that images and videos can be stored in greater quantities or for longer periods.

Australia also has one of the highest rates of mobile phone ownership in the world.[11] Children have extensive access, with around a third of children between the ages of 5 and 14 having access to their own mobile phone.[12] Mobile phones themselves come with features including cameras to capture still and moving images, music players and recording capabilities. Their unobtrusiveness and prevalence means that it is possible for people to be photographed or recorded without their knowledge almost anywhere.

---

[9] *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479 at 494 (Latham CJ).
[10] Australian Bureau of Statistics, *Household Use of Information Technology, Australia, 2008-09* (catalogue no. 8146.0) (released 16 December 2009) available at <www.abs.gov.au> (viewed 16 August 2011).
[11] See Australian Government, *About Australia: Information and Communications Technology* (2008) available at <www.dfat.gov.au/facts/ict.html> (viewed 16 August 2011).
[12] See Australian Bureau of Statistics, above n 10.

Australians are increasingly connected to the internet at home and at work. At the end of 2010 there were more than 10 million internet connections with an Internet Service Provider (ISP), and unknown numbers of people at the end of those connections.[13] This number of internet connections has increased by 16.7% between December 2009 and December 2010.[14] In 2008-09 the Australian Bureau of Statistics (ABS) found that 72% of households had access to the internet at home.[15] In only a decade it had more than quadrupled from 16%.[16] Of the 2.7 million children aged 5 to 14 years in 2009, 79% used the internet.[17].

The Australian Bureau of Statistics has only recently started releasing data relating to wireless internet connections via a mobile handset, but between June 2010 and December 2010 there was a 21% increase in the number of mobile handset internet subscribers in Australia – some 8.2 million handsets.[18]

The proportion of Australian businesses with access to the Internet has also increased, from 71% to 87% over the five years from 2002-03 to 2007-08.[19]

Australians are demanding access to faster internet speeds. In December 2009, 89% of internet connections were broadband connections according to the OECD definition of exceeding 256kbps[20], and 63% of internet connections had speeds greater than 1.5mbps.[21] A year later 81% of internet connections exceeded 1.5mbps.[22] With the Government's commitment to build the National Broadband Network (NBN) to provide 93% of Australian homes and businesses with access to a high-speed fibre network capable of providing speeds of up to 1 gigabit per second, and increasing delivery of health, education and government services online – the take up of greater speeds is only going to increase.

As the NBN rollout continues, there will be significant growth in the level of online activity, both in terms of the time people spend online and the amount of data they consume.

Between June 2005 and June 2010, the number of Australians using the internet more than 15 hours per week, doubled.[23] The proportion of people who used the internet at home and used it every day grew from 51% in 2007-08 to 58% in 2008-09.[24] Amongst children, the ABS

---

[13] Australian Bureau of Statistics, *Internet Activity, Australia, December 2010* (catalogue no 8153.0) (released 1 April 2011) available at <www.abs.gov.au> (viewed 16 August 2011).
[14] Ibid.
[15] See Australian Bureau of Statistics, above n 10.
[16] Ibid.
[17] Ibid.
[18] See Australian Bureau of Statistics, above n 13.
[19] Australian Bureau of Statistics, *Year Book Australia, Use of Information Technology, Australia, 2009-10* (catalogue no. 1310.0) (released 4 June 2010) available at <www.abs.gov.au> (viewed 16 August 2011).
[20] Kilobits per second.
[21] Megabits per second. See Australian Bureau of Statistics, above n 13.
[22] See Australian Bureau of Statistics, above n 13.
[23] See Australian Bureau of Statistics, above n 13.
[24] See Australian Bureau of Statistics, above n 19, under *How Australia Accesses and Uses the Internet*.

found that only 42% of children who used the internet at home used it for less than 2 hours per week, 17% used it more than 10 hours per week, and 4% were online for more than 20 hours per week.[25]

Between the December quarter 2009 and the December quarter 2010 there was a 50% increase in the amount of data downloaded.[26] The volume of data downloaded using mobile handsets increased by more than 500% from 717 (TB terabytes) in the June 2010 quarter to 4029 TB in the December 2010 quarter.[27] Mobile handset downloads also increased as a proportion of overall downloads from 0.5% in the June 2010 quarter to 2.1% in the December 2010 quarter.[28]

The percentage of Australian businesses with a web presence is growing – from 23% in 2002-03 to 36% in 2007-08.[29] Businesses primarily use the internet for financial activities (including online banking, invoicing and making payments), and to enable people to work from home or other locations.[30]

The recent proliferation of social networking sites allows extensive online networks to be created and maintained, for links and associations to be made, and for images and information to be widely shared.

The development of what has been called 'Web 2.0' or the 'collaborative web' has included the development of tools such as blogs, wikis and social networking platforms.[31] These tools encourage or require greater levels of engagement and interactivity and allow for greater amounts of data and opinion to be published than ever before.

Images, sounds and other information that is readily able to be recorded and stored can be easily uploaded onto social media websites, posted on the internet by blogging or micro-blogging, distributed over email, or by instant messaging.

Over the last decade, technology has clearly become integral to our engagement with government, business and each other.

Just as the daily social interactions of Australians have been altered fundamentally by the pervasiveness of these digital technologies, so too has the landscape for the preservation of

---

[25] Australian Bureau of Statistics, *Children's Participation in Cultural and Leisure Activities, Australia, 2009* (catalogue no. 4901.0) (released 28 October 2009) available at <www.abs.gov.au> (viewed 16 August 2011). See also Australian Bureau of Statistics, above n 10.

[26] See Australian Bureau of Statistics, above n 13.

[27] See Australian Bureau of Statistics, above n 13.

[28] Ibid.

[29] See Australian Bureau of Statistics, above n 23.

[30] Australian Bureau of Statistics, *Business Use of Information Technology, Australia, 2007-08* (catalogue no. 8129.0) (released 20 August 2009) available at <www.abs.gov.au> (viewed 16 August 2011).

[31] See Australian Government, *Engage: Getting on with Government 2.0 – Report of the Government 2.0 Taskforce* (2009) available at <http://gov2.net.au/report/>.

individuals' privacy. The speed and reach of the internet has the potential to facilitate the transmission of personal information to a previously unheralded audience.

However, technology can also safeguard individuals' privacy in this digital age. Increasingly, entities and organisations are taking steps and instituting policies to respond to the threats to privacy posed by such technological and commercial developments. Just as there is a need to be aware of challenges posed by these developments, there is also a need to increase awareness of how to utilise technological safeguards to limit individuals' and entities' exposure to privacy breaches.

In many cases, recordings of private information or collections of data are also handled in ways consistent with an entity's privacy policy, with the Commonwealth Privacy Act or with equivalent laws. Technologies are also being rapidly developed to allow the better protection of personal information and to help remedy the effects of identity theft or privacy invasion.

Websites are increasingly collecting and storing a variety of information – information relevant to particular customers or to their customer base generally. That may include, for example, information on previous purchases, information on the frequency and association of particular internet search terms, data on the rate of 'click through' for particular blast email or website-elements, or information on the length of time spent viewing particular web pages. That information may then be used for a variety of purposes: for example to target advertising or as an asset to be sold to other entities.

While these new and developing technologies, tools and software are enriching the lives, work and study of Australians in many ways, they may simultaneously be enabling (or making more easy) the communication and transmission of personal or sensitive data, images, information, or other details of a person's private life.

It may reasonably be observed that more information is being recorded and stored, that people are increasingly using social networking and other websites, and that recording technologies and devices are becoming cheaper and widely available.

As technology that can more easily be used to invade privacy develops, it becomes all the more appropriate to ask whether current privacy laws are adequate to protect personal privacy.

In light of the current privacy context, this paper is seeking views about whether the Australian Government should create a right for individuals to seek redress from another person who seriously invades their privacy.

In the event that there is to be such a right, the paper also asks in what circumstances this right should apply, and what remedies should be available.

1. *Do recent developments in technology mean that additional ways of protecting individuals' privacy should be considered in Australia?*

The present state of the law in Australia and other jurisdictions regarding a right to privacy

In Australia, there is no clear cause of action for invasion of privacy in statute or at common law. However, such a cause of action exists in New Zealand, the United States, Canada, the United Kingdom and the European Union, either in statute, or through development of the common law.[32]

Present state of the 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 recognising a tort of invasion of privacy.

The absence of the common law in this area can be traced back to 1937, where the High Court found in *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor*[33] that breach of privacy was not recognised in Australian law. This precedent was maintained by Australian courts for over 60 years. It was not until 2001 that the High Court, in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd,*[34] departed from this decision, clearly indicating that the decision in *Victoria Park* does not stand in the path of the development of a cause of action for invasion of privacy.[35] However, the High Court did not determine whether a cause of action exists, nor has it clearly articulated what the scope of such a cause of action might be.

Since the High Court considered the *Lenah Game Meats* case, the common law has remained undeveloped. Only two cases – *Grosse v Purvis*[36] and *Doe v Australian Broadcasting Corporation*[37] – have expressly recognised a common law right to an action for invasion of privacy.

In *Grosse v Purvis*, the Queensland District Court found a breach of privacy to have occurred as a result of the defendant stalking the plaintiff over a prolonged period. In this case, the court awarded aggravated compensatory damages and exemplary damages. After noting that the High Court in *Lenah Game Meats* had removed the barrier which the *Victoria Park* case posed, Skoien SDCJ took what he viewed as 'a logical and desirable step' and recognised 'a civil action for damages based on the actionable right of an individual person to privacy'.[38]

---

[32] The text in this section includes extracts from and draws upon relevant sections of the ALRC Report, the VLRC Report and the NSWLRC Report.

[33] *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479.

[34] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199.

[35] Ibid at [107] (per Gummow and Hayne JJ, with whom Gaudron J agreed).

[36] *Grosse v Purvis* [2003] QDC 151.

[37] *Doe v Australian Broadcasting Corporation* [2007] VCC 281.

[38] *Grosse v Purvis* [2003] QDC 151 at [442].

The Court in that case determined that the 'essential elements' of the action for invasion of privacy were:

a) a willed act by the defendant;

b) which intrudes upon the privacy or seclusion of the plaintiff;

c) in a manner which would be considered highly offensive to a reasonable person of ordinary sensibilities;

d) and which causes the plaintiff detriment in the form of mental psychological or emotional harm or distress or which prevents or hinders the plaintiff from doing an act which she is lawfully entitled to do.[39]

Skoien SDCJ also considered that while a public interest defence was available, it was not relevant in the particular case. The facts in this case meant that it was not necessary to consider whether a privacy cause of action would include negligent acts.

In *Doe v Australian Broadcasting Corporation*, the defendant broadcaster published in its afternoon and evening radio news bulletins information that identified a victim of a sexual assault – the plaintiff. In doing so, the defendant breached s 4(1A) of the *Judicial Proceedings Reports Act 1958* (Vic), which makes it an offence in certain circumstances to publish information identifying the victim of a sexual offence. Hampel J in the County Court of Victoria held that, in addition to breaching a statutory duty owed to the plaintiff by virtue of the *Judicial Proceedings Reports Act*, the defendant broadcaster and two of its employees were liable to the plaintiff in equity for breach of confidence, and in tort for invasion of privacy. In this case, although Hampel J did not 'attempt to formulate an exhaustive definition of privacy'[40] the 'unjustified publication of personal information'[41] was considered to constitute a breach of the plaintiff's privacy.

The Australian Capital Territory and Victoria have introduced bill of rights legislation. Section 12 of the *Human Rights Act 2004* (ACT) and section 13 of the *Charter of Human Rights and Responsibilities Act 2006* (Vic) recognise a right to privacy and reputation, both stating that:

Everyone has the right –

a) not to have his or her privacy, family, home or correspondence interfered with unlawfully or arbitrarily; and

b) not to have his or her reputation unlawfully attacked.

Both the ACT and Victorian legislation also recognise a right to freedom of expression. While there are mechanisms to promote the application of the legislation, neither of these Acts provide individuals with privacy protections that are able to be enforced in the same way as a cause of action would operate.

---

[39] Ibid at [444].

[40] *Doe v Australian Broadcasting Corporation* [2007] VCC 281 at [162].

[41] Ibid at [164].

United States

Nearly all US states now recognise a right to privacy, either at common law or, in a few states, as a creation of statute.

The *Second Restatement, Torts* states that privacy tort protection exists where:

1 One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person;

2 One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy;

3 One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public;

4 One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to the other for invasion of his privacy, if (a) the false light in which the other was placed would be highly offensive to a reasonable person, and (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed. [42]

The privacy torts are subject to the same defences that apply in the US to defamation. Such defences include an absolute parliamentary and court privilege; consent; and conditional privileges for other activities, such as reporting public proceedings and reasonable investigation of a claim against a defendant. The constitutional protections for freedom of speech and freedom of the press are also relevant in construing the US law.[43]

A successful claim of invasion of privacy under common law entitles the plaintiff to recover damages on three bases: the harm from the loss of privacy; mental distress reasonably suffered; and when there is cause for 'special damages'. It remains unclear whether damages can be awarded in the absence of proof of actual harm. Injunctions are not readily ordered.[44]

---

[42] See *Restatement of the Law, 2nd, Torts 1977* (US) at sections 652B-652D. The *Restatements* are expositions on the law on specific subjects (based on court decisions) published by the American Law Institute.

[43] See *Constitution of the United States*, First Amendment: 'Congress shall make no law ... abridging the freedom of speech, or of the press ...'.

[44] See VLRC Report at 139.

European Union

The *European Convention on Human Rights* (*ECHR*) contains a right to private and family life, home and correspondence.

Article 8 of the *ECHR* is expressed in the following terms:[45]

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 is in accordance with the law and is necessary in a democratic society in the interests 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 freedoms of others.

In *Von Hannover v Germany* the European Court of Human Rights established the benchmark from which an analysis of the application of Article 8 must proceed.[46] The Court recognised the 'fundamental importance of protecting private life from the point of view of the development of every human being's personality'.[47] The Court noted that the protection 'extends beyond the private family circle and also includes a social dimension ... anyone, even if they are known to the general public, must be able to enjoy a 'legitimate expectation' of protection of and respect for their private life'.[48]

The extent of 'private life' remains unclear following the *Von Hannover* decision.

---

[45] European *Convention for the Protection of Human Rights and Fundamental Freedoms* (Article 8—Privacy).

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

[47] Ibid at [69].

[48] Ibid.

United Kingdom

There is no freestanding right to privacy in the UK. The courts repeatedly have stated that 'English law knows no common law tort of invasion of privacy'.[49] Instead, the cause of action for breach of confidence has been extended to encompass misuse or wrongful dissemination of private information. Extensive expansion of the law in this area has occurred in recent years; however the law concerning the elements, defences and remedies that apply to the cause of action for misuse of private information is not yet settled.

The developments in the UK have been influenced in recent years by the *ECHR* and the *Human Rights Act 1998* (UK). The *Human Rights Act* incorporates (to some extent) the *ECHR* into the domestic law of the UK. The *Human Rights Act* came into force in October 2000. Since that time, the courts in the UK have been influenced by Article 8 of the *ECHR*, and by the jurisprudence of the European Court of Human Rights interpreting that article.

Elements of the Tort

When analysing whether the elements of the tort have been established in a case of unlawful publication of private information (which, to date, constitutes the majority of the case law in the UK), the court engages in a two-part balancing exercise. The court first ascertains whether the information is private 'in the sense that it is in principle protected by Article 8'. If the answer is 'yes', the court then asks, 'in all the circumstances, must the interest of the owner of the private information yield to the right of freedom of expression conferred on the publisher by Article 10'?[50]

The courts in the UK have avoided setting too high a bar when determining what 'private' means within the context of Article 8.[51] The elements of the cause of action appear to be, first, 'whether the claimant had a reasonable expectation of privacy in relation to the particular information in question' and, secondly, 'whether there is some countervailing public interest such as to justify overriding that prima facie right'.[52] Both issues are 'essentially questions of fact', but the courts have provided limited guidance about the matters to consider in resolving these questions of fact.[53]

When considering the first limb of the test, the person alleging a breach of Article 8 must establish that interference with private life was of 'some seriousness' before the article is engaged.

---

[49] *OBG Ltd v Allan; Douglas v Hello! Ltd* [2007] 2 WLR 920 at [272].

[50] *Ash v McKennitt* [2007] 3 WLR 194 at [11].

[51] ALRC Report at 2545.

[52] *The Author of a Blog v Times Newspapers Limited* [2009] EWHC 1358 (QB) at [7] (Eady J). An act of the defendant that led to the publication of the information in question appears to be subsumed within these two elements.

[53] *Murray v Big Pictures (UK) Limited* [2008] EWCA Civ 446 at [36] (Clarke MR).

Once the information is identified as 'private', the court must then 'balance the claimant's interest in keeping the information private against the countervailing interest of the recipient in publishing it'.[54]

Defences

The English courts have not yet articulated any defences to a claim for misuse of private information. It does appear, however, that consent is a defence, just as it is to most torts. There may also be a 'defence' that is quite similar to the defence of qualified privilege in defamation law. In *Campbell v MGN Limited,* all five Law Lords accepted that it was lawful for the newspaper in question to publish the fact that the appellant was a drug addict because she had made many public statements to the contrary.[55] Reporting that Narcotics Anonymous was treating her, and the details of that treatment, including a photograph of the plaintiff outside a Narcotics Anonymous premises, did, however, constitute an invasion of her privacy.

Proof of damages and remedies

It is not clear whether the wrong of misuse of private information requires proof of actual damage or whether, like the tort of trespass, it may be committed without proof of any damage. This lack of clarity has created uncertainty about the types of damages that may be awarded. Damages awards have generally been modest in these cases.[56] The British courts have also issued injunctions to prevent the initial publication, or continued publication, of material in some misuse of private information cases.

Even though damages awards have generally been quite small in misuse of private information litigation, costs awards have been more significant. The plaintiff in *Campbell* was awarded damages of £3 500 and costs of £1.08 million. In *Mosley v News Group Newspapers Limited* the plaintiff was awarded damages of £60 000 and costs of £850 000 when the defendant newspaper exposed his involvement in sexual activities involving a group of women and published details and video of the incident.[57] One man was awarded damages of £11 800 and costs of £18 075 for the broadcasting of CCTV footage of his suicide attempt.[58]

There have been a number of recent high-profile injunctions in the UK, which prevent the publication of information about celebrities (including some sports stars) which is confidential or private, or the publication of information about the existence of the relevant injunction, proceedings or orders.

---

[54] *Campbell v MGN Ltd* [2004] 2 AC 457 at [137].
[55] *Campbell v MGN Limited* [2004] 2 AC 457.
[56] VLRC Report at 132.
[57] *Mosley v News Group Newspapers Limited* [2008] EWHC 1777 (QB).
[58] *Peck v United Kingdom* [2003] ECHR 44.

Canada

There is no common law tort of invasion of privacy in Canada. However, four provinces—British Columbia (1968), Manitoba (1970), Saskatchewan (1974), and Newfoundland and Labrador (1981)—have statutory causes of action for invasion of privacy.[59]

Generally, the legislation provides that 'it is a tort, actionable without proof of damage, for a person wilfully and without claim of right, to violate the privacy of another person'.[60]

Elements of the Tort

The provinces have enacted three similar elements required to be proved to establish the tort. For example, the British Columbia Act states: 'The nature and degree of privacy to which a person is entitled in a situation or in relation to a matter is that which is reasonable in the circumstances, giving due regard to the lawful interests of others'.[61]

Secondly, all but the Manitoba Act require proof that the defendant acted wilfully. This means that the defendant knew, or ought to have known, that an act would violate the privacy of the plaintiff, and was not merely negligent.

Thirdly, the statutes require the courts to consider a range of relevant factors such as the nature of the privacy invasion and the relationship between the parties. With the exception of the Manitoba Privacy Act, which stipulates that an invasion of privacy must be 'substantial', the legislation does not require the alleged invasion of privacy to be 'serious' or 'highly offensive'.

Defences

All four Acts list exceptions or defences to the cause of action. The common exceptions or defences are:

- the plaintiff consented to the conduct;
- the defendant's conduct was incidental to the exercise of a lawful right of defence of person or property;
- the defendant's conduct was authorised or required by law;

---

[59] *Privacy Act 1996* RSBC c 373 (British Columbia); *Privacy Act* CCSM section P125 (Manitoba); *Privacy Act 1978* RSS c P-24 (Saskatchewan); *Privacy Act 1990* RSNL c P-22 (Newfoundland and Labrador).
[60] *Privacy Act 1978* RSS c P-24 (Saskatchewan) section 2. See also *Privacy Act 1996* RSBC c 373 (British Columbia) s 1(1); *Privacy Act* CCSM section P125 (Manitoba) section 2(1); *Privacy Act 1990* RSNL c P-22 (Newfoundland and Labrador) section 3(1). The British Columbia legislation differs from the statutes in force in the other provinces in that it also protects the unauthorised use of the name or portrait of another: *Privacy Act 1996* RSBC c 373 (British Columbia) section 3.
[61] *Privacy Act 1996* RSBC c 373 section 1(2).

- the defendant is a police or public officer who was engaged in his/her duty and the conduct was neither disproportionate to the matter being investigated nor committed in the course of a trespass; and
- if the defendant's conduct involved publication, the publication was privileged, fair comment or was in the public interest.

The Saskatchewan Privacy Act also contains a.defence of acting in the scope of newsgathering, while the Manitoba Act has a defence for a person who neither knows, nor reasonably should have known, that the act in question would violate the privacy of any person.

Proof of Damage and Remedies

The legislation creating a cause of action for invasion of privacy in the Canadian provinces expressly labels the cause of action a 'tort'. The statutes of British Columbia, Saskatchewan, Manitoba, and Newfoundland and Labrador providing for the tort of violation all specify that the tort is actionable without proof of damage.

The Canadian statutes, other than the British Columbia Privacy Act, specify the remedies that a court may order for an unlawful invasion of privacy. Common remedies are: damages; an injunction; an order for the defendant to account to the plaintiff for profits in consequence of the violation; and an order for the defendant to deliver the documents obtained in consequence of the violation.

Charter of Rights and Freedoms

While the *Canadian Charter of Rights and Freedoms 1982* does not specifically guarantee a right to privacy, the Supreme Court of Canada has interpreted the right in section 8[62] to include a reasonable expectation of privacy in relation to governmental acts. The province of Quebec has guaranteed 'a right to respect for ... personal life' in its *Charter of Human Rights and Freedoms*.[63]

---

[62] "Everyone has the right to be secure against unreasonable search or seizure."

[63] *Charter of Human Rights and Freedoms* RSQ c-12 (Quebec) section 5.

New Zealand

In *Hosking v Runting* a majority of the New Zealand Court of Appeal recognised a common law tort of privacy.[64]

While the majority stressed that 'the cause of action will evolve through future decisions as courts assess the nature and impact of particular circumstances', the Court was prepared to extend tort protection to wrongful publicity given to private lives.[65] The Court was influenced by the third formulation of the United States privacy tort,[66] and the New Zealand tort is similar to that which falls within the UK extended cause of action for breach of confidence for misuse of private information.[67]

The Court found that there are two fundamental requirements for a successful claim for interference with privacy:

1. [t]he existence of facts in respect of which there is a reasonable expectation of privacy; and
2. [p]ublicity given to those private facts that would be considered highly offensive to an objective reasonable person.[68]

The majority of the Court in *Hosking v Runting* suggested that there should be a defence of legitimate public concern in order to ensure that 'the scope of privacy protection should not exceed such limits on the freedom of expression as is justified in a free and democratic society'.[69] The use of the term 'public concern' rather than 'public interest' reflected the Court's view of the difference between 'matters of general interest or curiosity to the public, and matters which are of legitimate public concern'.[70]

The precise status of the New Zealand tort of invasion of privacy by publishing private facts is uncertain because some members of that country's highest court, the Supreme Court, have cast doubts upon its continued acceptance and content. In one case, Anderson J, who was one of the two dissenting judges in *Hosking v Runting*, said that, in his view, the existence of the tort and its scope were matters for debate in the Supreme Court.[71] Chief Justice Elias queried the details of the tort, particularly the need for the second element concerning the 'highly offensive' nature of the publicity.[72]

---

[64] *Hosking v Runting* [2005] 1 NZLR 1.
[65] Ibid at [118].
[66] See page 15.
[67] See pages 17-18.
[68] *Hosking v Runting* [2005] 1 NZLR 1 at [117].
[69] Ibid at [130].
[70] Ibid at [133] (Gault and Blanchard JJ). See further VLRC Report at 156-159.
[71] *Rogers v Television New Zealand Ltd* [2008] 2 NZLR 277 at [144] (SC).
[72] Ibid at [25].

There have been relatively few cases in New Zealand dealing with the tort of invasion of privacy by publishing private facts since developments started at the trial court level in the mid-1980s. The VLRC Report stated in 2010 that it 'appears that 'fifteen people have brought cases wholly or partly based on privacy, and many of them have been neither rich nor famous'. Damages were ordered in only two cases, with the highest award being NZ$25 000. An injunction restraining publication was granted on five occasions.[73]

The New Zealand Law Commission recently recommended that development of the tort recognised in *Hosking v Runting* should be left to the common law.[74] Although the Commission acknowledged that a statutory cause of action would make the law more accessible and certain, it referred to the absence of 'evidence that the current state of the law is causing practical difficulties to anyone'.[75]

---

[73] VLRC Report at 136 (citations omitted). Note also New Zealand Law Commission, *Invasion of Privacy: Penalties and Remedies Review of the Law of Privacy Stage 3*, Issues Paper No 14 (2009).
[74] New Zealand Law Commission, *Invasion of Privacy: Penalties and Remedies, Review of the Law of Privacy Stage 3*, Report No 113 (2010) at 91.
[75] Ibid at 90.

Is there a need for a statutory cause of action for serious invasion of privacy in Australia?

This section invites comment on whether a statutory cause of action for serious breach of privacy should be introduced in Australia.[76] It discusses the considerations the law reform commissions thought relevant to the question of whether such a reform was desirable. It then turns to whether evolution of the common law or new legislation provides the most appropriate vehicle for development of the law in this area.

The ALRC was the first Australian law reform commission to consider whether or not there was a need for a cause of action for serious invasion of privacy.[77] It considered this question in light of the recommended broader reforms to privacy law and practice.

Following an extensive community consultation exercise,[78] the ALRC recommended that the Government legislate for a right to sue, stating that there was 'strong support for the enactment of a statutory cause of action for a serious invasion of privacy' in Australia.[79]

The NSWLRC[80] and VLRC[81] came to the same conclusions (though the latter recommended two causes of action – for misuse of information and interference in seclusion).

This paper now turns to discuss some of the arguments in favour of and against a statutory cause of action.

Existing protections: comprehensiveness and adequacy

Some stakeholders have argued that existing laws and industry codes of conduct adequately protect privacy in Australia. However, the 'gap-filling' role of a statutory cause of action for the most serious privacy invasions has also been widely acknowledged.

Existing privacy (data protection) legislation in the Commonwealth, States and Territories, general law actions and remedies, industry codes of practice, and a range of voluntary privacy initiatives each play their part in the present privacy protection framework in Australia. However, as far as this framework does not cover every circumstance, or provides insufficient remedies, the ALRC concludes there are 'gaps' in the protection provided to individuals and their private lives.

---

[76] A cause of action may be understood as a legal right to sue another party to obtain particular 'remedies', such as damages or court declarations, in respect of an enforceable claim against that other party.

[77] See ALRC Report at 2564 *passim*.

[78] Which included, for example, some 250 meetings and the receipt of 585 submissions: see further NSWLRC Report at 7-8.

[79] ALRC Report at 2557.

[80] See NSWLRC Report at 8-10. See further NSWLRC Report at 7-22 and VLRC Report at 145-146.

[81] See VLRC Report at 147.

Those gaps arise, for example, because the Commonwealth Privacy Act has as its focus information privacy and data protection, rather than privacy protection more broadly. That Act, and some State and Territory privacy legislation, also make only certain types of remedies available, or those remedies are available only against particular entities or types of entities, or only after particular procedural steps have been followed (eg after notification to the entity or to the Information Commissioner).

The tort of trespass, and statutory actions for defamation, have their own rules, requirements and exclusions. These limit the scope and application of these bodies of law where particular *privacy* invasions have occurred. To take one example referred to by the ALRC, the equitable action for breach of confidence is:

> presently confined to cases involving the use of information of a private nature, whether in word or pictorial form. So, however strong and understandable may be the feeling of harassment of a person who is hounded by photographers when carrying out activities of a private nature, and however unacceptable the behaviour of the pack, there will be no cause of action until an intrusive photograph is published.[82]

The VLRC pointed to a different kind of gap in its report:

> There is a clear gap in the current regulatory regime. Although the criminal law deals with the most offensive invasions of privacy, there is no parallel civil cause of action for people harmed by that behaviour. ... The Victorian Privacy Commissioner informed the [VLRC] that people contact her office with complaints about interferences with spatial privacy or misuse of private information for which for there is no redress under Victorian and Commonwealth law.[83]

The Commonwealth Office of the Privacy Commissioner, in its 2007 submission to the ALRC consultation process, stated that:

> a dedicated privacy based cause of action could serve to complement the already existing legislative based protections afforded to individuals and address some gaps that exist both in the common law and legislation.[84]

Other legal remedies or mechanisms may provide more appropriate methods to protect privacy or influence behaviour than a civil mechanism such as the proposed cause of action. For example, criminal laws (and sanctions such as imprisonment), or data protection laws (and sanctions such as monetary fines), may be more appropriate to deter particular types of conduct than a civil cause of action.

---

[82] See ALRC Report at 2564, referring to the UK common law, and quoting Sir Roger Toulson, 'Freedom of Expression and Privacy' (Paper presented at the Association of Law Teachers Lord Upjohn Lecture, London, 9 February 2007), at 7.

[83] VLRC Report at 147.

[84] Office of the Privacy Commissioner, *Submission PR 499* [to the ALRC privacy review], 20 December 2007; cited in ALRC Report at 2557.