PRIVACY, BUSINESS AND THE DIGITAL ERA

Address to New South Wales Law Society
Continuing Professional Development Seminar Series

The Honourable Justice Ruth McColl AO
Court of Appeal
Supreme Court of New South Wales

Sheraton on the Park

8 March 2014[1]

Introduction

1 In June 2011, International Data Corporation (IDC) which describes itself as the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets[2] announced that data creation was occurring at a record rate. It said that in 2010, the world generated over 1ZB[3] (zettabyte) of data; and forecast that by 2014 that figure would grow to 7ZB a year. To give you an idea of what that means in real terms, 7 Zettabytes is the equivalent of:

- 1,750 billion DVDs
- 252 million years of HD video
- 4,949 trillion copies of the more than 2,000 page US Patient Protection and Affordable Care Act (Obamacare). Stacked end to end, the documents would stretch from Earth to Pluto and back 112 times

2 IDC attributed "[m]uch of this data explosion" to what it described as "a dramatic increase in devices located at the periphery of the network including embedded sensors, smartphones, and tablet computers". It explained that this data created "new opportunities to 'extract more value' in human genomics, healthcare, oil and gas, search, surveillance, finance,

and many other areas" and proclaimed that "[w]e are entering the age of 'Big Data'.[4]

3 What does this Orwellian sounding concept, "big data" mean?

4 According to one interpretation:

> "Big Data is the tracking and aggregation of a large volume of data (including personal information) from search engine histories, emails, sale transaction histories, reward/loyalty programs, app downloads and the like. The aggregation, tracking and analysis of large volumes of data across such a range of variables is of considerable value to business, allowing business to gain insight into its consumers and the market, making it more responsive, increasing efficiency and encouraging new offerings for 'new' markets. As well as using their own data, businesses are also finding more and more ways of combining their data with that of third parties in order to analyse more variables…"[5]

5 Like some who inhabited Orwell's futuristic world of "1984" (now very much in the past) not all members of the digital community (which I assume includes just about everybody here) is sanguine about this potential invasion of their privacy or as appreciative of its commercial value.

6 On European Data Protection Day 2014, 28 January 2014, just 7 or so weeks ago, Vice-President Reding of the European Commission called for a new data protection compact for Europe intended to strengthen privacy rights and boost Europe's digital economy. She identified the need for that compact as arising in the following circumstances:

> "Data is the currency of the digital age. Data is used by all businesses - from insurance firms and banks to social media sites and search engines. In a globalised world, the transfer of data to third countries has become an important factor in daily life. There are no borders online and cloud computing means data might be sent from Berlin to be processed in Boston and stored in Bangalore…[W]ith surveillance revelations making the headlines almost on a daily basis, many people are not confident about giving out their personal data. 92% of Europeans are concerned about mobile apps collecting their data without their consent. And 89% of people say they want to know when the data on their smartphone is being shared with a third party."[6]

7 Here is a micro-illustration of how what I will term data mining by businesses is invading individual's privacy.

8 A Minneapolis man discovered his teenage daughter was pregnant because coupons for baby food and clothing were arriving at his address from what it described as "the US superstore Target". The girl, who had not registered her pregnancy with the chain, had been identified by a system that looked for pregnancy patterns in her purchase behaviour.[7]

9 So what is data mining? It is a buzzword describing "…the process of analysing data from different perspectives and summarizing it into useful information - information that can be used to increase revenue, cuts costs, or both. …Technically, data mining is the process of finding correlations or patterns among dozens of fields in large relational databases."[8]

10 Every time you swipe your Flybuys or Everyday Rewards Card, you are giving the business where you are shopping valuable information about yourself which can be gold in the data mining stakes.

11 When you use your computer or smartphone to undertake a search, you leave "a footprint of [your] interests, relations, and intentions [which] … can be subsequently used both for commercial purposes and as a result of requests and fishing operations and/or data mining by law enforcement authorities or national security services".[9]

12 Here's another example (for some reason all these examples are from the USA):

> "[O]ne Midwest grocery chain used the data mining capacity of Oracle software to analyse local buying patterns. They discovered that when men bought [nappies] on Thursdays and Saturdays, they also tended to buy beer. Further analysis showed that these shoppers typically did their weekly grocery shopping on Saturdays. On Thursdays, however, they only bought a few items. The retailer concluded that they purchased the beer to have it available for the upcoming weekend. The grocery chain could use this newly discovered information in various ways to increase revenue. For

> example, they could move the beer display closer to the [nappy] display. And, they could make sure beer and [nappies] were sold at full price on Thursdays."[10]

13 So these are some obvious ways business can entrench on our privacy in the digital world. You may think they're relatively innocuous (save to the extent we don't get bargains at the supermarket), but there are, of course, more disturbing examples.

14 I do not, I am sure, need to remind you about what gave rise to the Leveson Inquiry in the United Kingdom. It was charged with investigating the role of the press and police in the phone-hacking scandal, and sparked by public revulsion about a single action – the hacking of the mobile phone of a murdered teenager.[11] The phone-hacking was said to have taken place in a context in which the newspaper, *News of the World*" displayed a "casual attitude to privacy".[12]

15 So how has it come to this: that businesses can plunder information revealed by our shopping habits or our personal digital devices with, it might seem, little or no concern about our privacy and, in the Leveson Inquiry situation, the extent to which their conduct trespassed upon a serious Police investigation?

Outline of paper

16 This paper is intended to look at how, and whether, the common law and statute protect Australians' privacy in the digital world, as well as how other jurisdictions have approached these issues.

17 It is intended to contextualise the extent to which, if at all, our privacy is protected from business scrutiny.

18 What will become apparent is that Australia lags behind other common law jurisdictions in terms of the development of a common law cause of action to protect individual privacy. Further, despite many law reform inquiries

and correlative recommendations, politicians appear to have consistently baulked at the notion of introducing a statutory cause of action affording such protection. And, despite reforms to legislation dealing with information collection by government and business, there are still gaps in our privacy protection.

19 This may have been appropriate at a time when incursions on individual privacy were relatively minor, but can it any longer be sustained in the digital era when, as my introduction has outlined, the creation of personal data is increasing exponentially?

What is privacy?

20 But first, what is privacy? Is it a "right to be let alone", a "right to be forgotten" or does it matter any more?

21 Privacy has been described as " …as a value [which] … is important for individuals to live a dignified, fulfilling and autonomous life". It is said to be "an important element of the fundamental freedoms of individuals which underpin their ability to form and maintain meaningful and satisfying relationships with others; their freedom of movement and association; their ability to engage in the democratic process; their freedom to advance their own intellectual, cultural, artistic, financial and physical interests, without undue interference by others."[13]

22 However, as Gleeson CJ has said:

> "[42] 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 relationships, or

> finances, may be easy to identify as private; as may certain kinds of activity, which a reasonable person, applying contemporary standards of morals and behaviour, would understand to be meant to be unobserved. The requirement that disclosure or observation of information or conduct would be highly offensive to a reasonable person of ordinary sensibilities is in many circumstances a useful practical test of what is private."[14]

23 In his typically pithy way, his Honour has encapsulated some of the dilemmas which have confronted courts looking to carve out an express common law cause of action conferring a right of privacy, at least in this country.

24 Last year, debate about privacy, both in Australia and overseas, has focused on information privacy in the digital era in the context of "the rapidly expanded technological capacity of organisations to track the physical location and activities of individuals, to collect and use information from social media, to aggregate data from many sources, and to intercept and interpret the details of communications".[15] This, as shall become apparent, has led to renewed focus on the possible enactment of a statutory cause of action for invasion of privacy.

25 In contrast, a common law right of privacy has been recognised in the USA for close to a century. Both the United Kingdom and New Zealand recognise a tort of misuse of private information and a tort of intrusion upon seclusion: *Vidal-Hall v Google* [2014] EWHC 13 (QB); *Hosking v Runting* (2004) 7 HRNZ 301; (2005) 1 NZLR 1 (photographs taken for commercial purposes in public street of infant children of a well-known television personality); *C v Holland* [2012] NZHC 2155 (Secret videos of woman in shower).

26 How has it come to this? Do we have "a right to be left alone", a "right to be forgotten" or does anyone really care?

A bit of history

27 The first port of call in the common law world is the USA. And as will be apparent, everything old is new again.

28 In 1890, Samuel Warren, a lawyer, and Louis Brandeis, who later was appointed a justice of the United States Supreme Court, published an essay, "The Right to Privacy", in which they described the principle that the individual should have "full protection in person and in property" as being as "old as the common law". But, they continued:

> "[I]t has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society."[16]

29 The essay called for the common law to recognise a "right to be let alone"[17], a right which could be invoked to protect the privacy of an individual.

30 What prompted this call? Well, in terms redolent of the current debate, Warren and Brandeis complained that:

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual … the right 'to be let alone.' Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.' For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of the invasion of privacy by the newspapers, long keenly felt…
>
> The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him

> to mental pain and distress, far greater than could be inflicted by mere bodily injury."[18]

31 Warren and Brandeis sought to identify the limitations of the right to privacy they proposed and what remedies might be granted for its enforcement. They accepted that determining in advance of experience the exact line at which the dignity and convenience of the individual must yield to the demands of the public welfare or of private justice would be a difficult task; but thought general rules could be found by analogy with the law of slander and libel, and in the law of literary and artistic property.[19] They formulated some guiding principles but, critically, were of the view that the right to privacy should "cease[s] upon the publication of the facts by the individual, or with his consent".[20]

32 The essay has been described as "inventing" the right to privacy[21], even though a large part of it was devoted to demonstrating how the right was embedded in existing common law rights.

33 Time does not permit me to trace the consequent development of the law.

34 Suffice it to say that a right of privacy is now accepted in the United States, the broad categories of which were identified in Prosser's classic statement in his article on "Privacy", published in 1960 as being[22]:

> "1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
>
> 2. Public disclosure of embarrassing private facts about the plaintiff.
>
> 3. Publicity which places the plaintiff in a false light in the public eye.
>
> 4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness."[23]

35 These categories have been accepted by the United States Supreme Court in *Time Inc v Hill* [1967] USSC 11; 385 US 374 (at 383) (1967); *Cox Broadcasting Corporation v Cohn* [1975] USSC 44; 420 US 469 (at 488)

(1975)] and in the *Restatement of the Law Second, Torts* [Section 652A]."[24]

United Kingdom

36 Like Australia to which I will come, and unlike the United States of America, "there is no over-arching, all-embracing cause of action for "invasion of privacy" in the United Kingdom either.[25] However, it was possible to say in 2004 that "protection of various aspects of privacy is a fast developing area of the law".[26]

37 Developments in the UK have largely flowed from extending the cause of action for breach of confidence to misuse or wrongful dissemination of private information, not least because English law is said to have been "unwilling, perhaps unable, to formulate any such high-level principle" as seen in the United States concept of "invasion of privacy".[27] However, it has recognised that there are "gaps; cases in which the courts have considered that an invasion of privacy deserves a remedy which the existing law does not offer" and some of which "can be filled by judicious development of an existing principle"[28].

38 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.

39 However, English law has now developed to the extent where it recognises a tort of misuse of private information. This is apparent from a recent case which demonstrates the potential availability in that jurisdiction for a private remedy for invasion of privacy, helpfully in relation to data mining and by

one of the largest search engine providers in the world (perhaps outside China).

40 In *Vidal-Hall v Google* [2014] EWHC 13 (QB) three claimants, residents of England and Wales, wished to bring proceedings against Google, a company incorporated in Delaware and based in California, in respect of damage they claimed they had suffered by reason of the fact that the information collected from their computer devices was used to generate advertisements which were displayed on their screens (i.e. targeted advertising based on their Google searches).

41 The specific heads of claim were for, relevantly, misuse of private information, and a statutory claim under the *Data Protection Act 1998* (UK). The damage the claimants said they suffered was acute distress, because their targeted advertisements might reveal sensitive information about themselves. In particular, they were concerned (see [22]):

> "… that [information] Google Inc collected from their computers or other devices used to access the internet … were forming the basis for advertisements targeted at them, … [and] that, as a result of such targeted advertisements, such matters had in fact, or might well have, come to the knowledge of third parties who they had permitted to use their devices, or to view their screens."

42 The claimants were granted permission by a Master to serve the claim form on Google Inc in Mountain View, California. Google Inc applied to this court for an order declaring that the English court had no jurisdiction to try these claims, and to set aside service of the claim form. Whether its application was successful turned in part on whether the claimants had a "good arguable case" in relation to each ground relied upon: (at [14]).

43 The judgement sets out in some detail the pleading of technical matters underpinning how Google's operations impinged on the claimants' privacy. I leave it to you to read the judgment, if you wish, to see how that may work.

44 Mr Justice Tugendhat therefore had to consider whether misuse of private information was a tort for the purposes of allowing service outside the jurisdiction. He concluded that it was, citing (at [67]) Lord Nicholls in *OBG Ltd v Allan* and *Douglas v Hello!* [2008] 1 AC 1 (at [255]) as follows:

> "As the law has developed breach of confidence, or misuse of confidential information, now covers two distinct causes of action, protecting two different interests; privacy, and secret ("confidential") information. It is important to keep these two distinct. In some instances information may qualify for protection both on grounds of privacy and confidentiality. In other instances information may be in the public domain, and not qualify for protection as confidential, and yet qualify for protection on the grounds of privacy."

45 Tugendhat J also referred (at [68]) to :

> "… a number of cases in which misuse of private information has been referred to as a tort consistently with *OBG* and these cannot be dismissed as all errors in the use of the words 'tort': Secretary of *State for the Home Office v British Union for the Abolition of Vivisection* [2008] EWHC 892 (QB), Eady J at para [28]; *Imerman v Tchenguiz* [2011] Fam 116 Lord Neuberger MR at para [65] ('there is now a tort of misuse of private information'); *Walsh v Shanahan* [2013] EWCA Civ 411 Rimer LJ at para [55] ('The tort for which Mr Walsh sued was, as Lord Nicholls of Birkenhead explained in *Campbell v Mirror Group Newspapers Ltd*…, paragraph 14, one which had firmly shaken off the limiting constraint of the need for an initial confidential relationship and was 'better encapsulated now as misuse of private information'."

46 Accordingly he concluded (at [70]) that the tort of misuse of private information was a tort for relevant purposes.

47 There is much more in the judgment on the issue of whether service should be set aside which does no touch upon the issue raised by this paper, but finally I would note that his Honour rejected (at [115] a submission by Google that "Browser-Generated Information" was not private. As his Honour found this (at [116]), "a surprising submission to be made on behalf of Google Inc", observing that "[i]It would not collect and collate the information unless doing so enabled it to produce something of

value [which was] the facility for targeted advertising of which the Claimants complain, and which yields the spectacular revenues for which Google Inc is famous".

Australian developments

48 Unlike the USA, Australia has not developed an "over-arching, all-embracing cause of action for invasion of privacy"[29], nor any express cause of action that might be said to find reflection in one of Prosser's four categories identified, nor a tort of misuse of private information such as has been recognised in the UK. Attempts to do so have been faltering, to say the least.

49 The only two cases decided by the High Court of Australia which have considered a "right of privacy" expressly were decided 64 years apart. Ironically, both were attempts by businesses to protect their business information.

50 In the first, *Victoria Park Racing and Recreation Ground Co Limited v Taylor* [1937] HCA 45; (1937) 58 CLR 479, the proprietors of a racecourse sought an injunction to restrain the broadcasting by a radio station of reports of races taking place on the plaintiff's racecourse. The reports were obtained from an observer who was stationed on a high platform erected on land adjoining the racecourse by the defendants, from which he could see what was happening on the racecourse and read the information which appeared on notice boards on the course as to the starters, scratchings, &c., and the winners of the races. A commentator stood on the platform and using a telephone transmitted to the radio station comments about, and descriptions of the races and announced the names of the winning horses. Attendances at the racecourse declined after the broadcasts commenced. The plaintiff's claim, under the head of nuisance was based, in part, on an argument that the law recognised a right of privacy that the defendant had infringed. The High Court by majority (Latham CJ, Dixon and McTiernan JJ; Rich and Evatt JJ dissenting) held

that the defendants had not infringed any legal right of the plaintiff. Time does not permit me to dwell upon the reasons of the individual justices. I will just briefly mention that Latham CJ observed (at 496) that while:

> "…no doubt the owner of a house would prefer that a neighbour should not have the right of looking into his windows or yard, but neither this court nor a court of law will interfere on the mere ground of invasion of privacy; and a party has a right even to open new windows, although he is thereby enabled to overlook his neighbour's premises, and so interfering, perhaps, with his comfort".

51 On the other side of the picture, one of the dissentients, Rich J (at 505) foreshadowed that the advance of television "may force the courts to recognize that protection against the complete exposure of the doings of the individual may be a right indispensable to the enjoyment of life."

52 During the time which elapsed between *Victoria Park* and the next High Court case dealing with a right of privacy, two reports of the Australian Law Reform Commission (the "ALRC")[30], written when Justice Michael Kirby was its chairman, accepted that such a tort could not be developed at common law while *Victoria Park* stood and recommended, albeit fruitlessly, legislative action instead.[31]

53 In *Australian Broadcasting Corporation v Lenah Game Meats* [2001] HCA 63; (2001) 208 CLR 199 ("*Lenah Game Meats*"), Lenah, which had a licence to take and hold brush tail possums from the Tasmanian Department of Parks, Wildlife and Heritage and had all approvals and licences necessary to carry on the business of killing, processing and exporting possums, complained that persons unknown to it unlawfully entered its premises, filmed aspects of its brush tail possum processing operations, and that Animal Liberation Ltd ("Animal Liberation") gave a video tape of that film to the ABC. Lenah sought an injunction to restrain the ABC from broadcasting that film arguing, inter alia, that for the ABC to engage in the activity would constitute an actionable invasion of its right to ''privacy''.[32]

54 Unlike the majority view in *Victoria Park*, the judgments in *Lenah Game Meats* did not shut the door to the development of the common law in a manner which might reflect underlying principles of privacy, rather they left that door at least ajar. However their Honours did not, with the exception of Callinan J, embrace the development of a tort of privacy *per se* but contemplated that if the law were to develop in that direction, it might do so by the development of existing principles. Even so, they also recognised the difficulty of formulating an independent concept of privacy, rather than recognising privacy interests through existing causes of action and their development.

55 I will not attempt to detail the reasons of each justice. However, here is a summary which undoubtedly does not do their Honours justice.

56 First, a majority, accepted in obiter statements that Australian law may recognise, albeit cautiously either through the development of existing causes of action or possibly as an independent cause of action, "principles [to] protect[] the interests of the individual in leading, to some reasonable extent, a secluded and private life, in the words of the [Restatement of the Law Second, Torts], 'free from the prying eyes, ears and publications of others' ".[33]

57 Secondly, of the majority, all recognised the difficulty of formulating an independent concept of privacy, rather than recognising privacy interests through an existing cause(s) of action and/or its (their) development.

58 Thirdly, their Honours were cautious about taking guidance from the United States law, having regard to the powerful effect in that jurisdiction of the First Amendment to the Constitution.

59 Fourthly, and interestingly, views were somewhat divided on the question whether a corporation might have a right of privacy. Gummow and Hayne JJ (with whom it will be recalled Gaudron J agreed) were adamant that such a right could not benefit a corporation. Kirby J appeared tentatively inclined to that view. However while Gleeson CJ observed (at [43]) that

"the foundation of much of what is protected, where rights of privacy, as distinct from rights of property, are acknowledged, is human dignity [and that] [t]his may be incongruous when applied to a corporation", he noted, as Callinan J did, that United Kingdom legislation recognised the possibility of a corporation having such a right (referring to *R v Broadcasting Standards Commission; Ex parte British Broadcasting Corporation* [2001] QB 885 (at 896-897)), and added that "[s]ome forms of corporate activity are private", noting that neither "members of the public, nor even shareholders, are ordinarily entitled to attend directors' meetings".

60 Fifthly, there is a majority of views in favour of the proposition that *Victoria Park* does not inhibit the development of a law of privacy.

61 *Lenah Game Meats* represents the last statement by the highest court in Australia about a possible tort of privacy.

Existing legislation

62 So what is the statutory position concerning our right of privacy?

63 The *Privacy Act 1988* (Cth), as well as 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. Other laws too many to mention, but which include the law of defamation, breach of confidence and trespass, also afford some measure of privacy protection.

64 When he launched the Australian Law Reform Commission's 2008 report titled *For Your Information; Privacy Law and Practice*, Senator John Faulkner said that the government would deal with the recommendations in two stages, the first of which would focus on unified privacy principles (which refers to recommendation 18-2 that the *Privacy Act 1998 (Cth)* should be amended to consolidate the current Information Privacy Principles (that currently apply to Australian Government agencies) and

National Privacy Principles (that currently apply to certain businesses) into a single set of privacy principles, referred to in this Report as the model Unified Privacy Principles.

65 He was true to his words.

66 In 2012 the Privacy Act 1988 was reformed, by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012* ("Privacy Amendment Act"), which was introduced to Parliament on 23 May 2012 and was passed with amendments on 29 November 2012. The changes will commence on 12 March 2014, next Wednesday. How's that for timing?

67 In the second reading speech Nicola Roxon, Attorney-General, described the Privacy Amendment Bill as one of the most significant developments in privacy reform since the *Privacy Act* was introduced in 1988.

68 The Act was formulated, according to the Attorney-General, with the challenges of the digital era in mind to address the fact that "[i]n an online world, we are increasingly sharing our personal information on social networking sites and paying our bills and buying footy tickets over the internet" such that there is a need to tighten "the rules around how companies and organisations can collect, use and disclose personal information."[34]

69 Among the changes introduced by the Privacy Amendment Bill are the "Australian Privacy Principles" – the APPs, which are a consolidation of the Information Privacy Principles and National Privacy Principles previously applicable into a single set of privacy principles". The APPs apply to both the private and public sectors.

70 There are 13 new APPs, which will apply to what are described as APP entities, namely "organisations" and Australian Government agencies.

71 The APPs deal with, inter alia, the collection of personal and sensitive information, and how to deal with such information.

72 " '[P]ersonal information' means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion: s 6.

73 "[S]ensitive information" has an extensive definition and includes information or an opinion about an individual's racial or ethnic origin; or political opinions; or membership of a political association; religious beliefs or affiliations; membership of a professional or trade association or a trade union, or sexual preferences or practices; criminal record, or health information or genetic information as long as, in all cases, the information also falls within the definition of personal information: s 6.

74 An APP entity must have a clearly expressed and up-to-date policy (the "APP privacy policy") about the management of personal information by the entity: APP 1.3. The policy must make clear how an individual may complain about a breach of the Australian Privacy Principles or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint; whether the entity is likely to disclose personal information to overseas recipients and if so, the countries in which such recipients are likely to be located, if it is practicable to specify those countries in the policy: APP1.4.

75 The APP's are, as you can imagine, very detailed and require close scrutiny. However an overview of those which might be seen as most relevant to business operators and individuals reveals the following:

(1) An "organisation (which will include most businesses other than small business operators), must not collect personal information (other than sensitive information) unless the

information is reasonably necessary for one or more of the entity's functions or activities **(APP 3.1).**

(2) An organisation must not collect “sensitive information” about an individual unless the individual consents to the collection of the information and the information is reasonably necessary for one or more of the organisation’s functions or activities **(APP 3.3).**

(3) If an organisation collects personal information about an individual, it must take such steps (if any) as are reasonable in the circumstances to notify the individual of that fact **(APP 5.1).**

(4) If an organisation holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless, inter alia, the entity has the consent of the individual or the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose (**APP 6**).

(5) If an organisation holds personal information about an individual the organisation must not use or disclose the information for the purpose of direct marketing, subject to certain exceptions, which essentially are that the individual would expect the organisation to use the information for that purpose, and that there is a clear opt-out process which has not been used **(APP 7).**

(6) Before an APP entity discloses personal information about an individual to a person who is overseas, the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australia Privacy Principles in relation to that information **(APP 8).**

(7) If an APP entity holds personal information about an individual and the entity no longer needs the information for any purpose for which the information may be used the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified **(APP 11).**

76 An individual may complain to the Australian Information Commissioner about an act or practice that may be an interference with the privacy of the

individual: s 36. If a complaint is made, the Commissioner is required to investigate the act or practice except in certain circumstances: s 40, Part V, "Investigations". If the Commissioner makes a determination sustaining the complaint, which may include a determination the complainant is entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice the subject of the complaint (s 52), that determination can be enforced by the complainant or the Commissioner in either the Federal Court or the Federal Circuit Court: s 55A.

77 The amendments will also give the Australian Information Commissioner enhanced powers, including the ability to:

(8) Accept enforceable undertakings the entity will take specified action directed towards ensuring that the entity does not do an act, or engage in a practice, in the future that interferes with the privacy of an individual: s 33E.

(9) Seek civil penalties in the case of serious and repeated breaches of privacy (s 13G).

78 These provisions go a long way it might be thought to regulating the manner in which businesses encroach on individuals' privacy. But do they go far enough?

The changing scene

79 Even the government clearly thinks the rapid advance of technology means there are still steps to be taken.

80 In 2011, when it might have been thought the 2012 amendments were in the pipeline, the Australian government, harking back to *Victoria Park*, recognised that developments in technology meant that it was more difficult for individuals to take steps to protect their own privacy by the mere erection of a higher fence. The Department of the Prime Minister and Cabinet published an Issues paper about a *Commonwealth Statutory Cause of Action for Serious Invasion of Privac*y, September 2011,

intended to inform its response to the Australian Law Reform Commission's recommendations to introduce a statutory cause of action for serious invasions of privacy. It recognised that "[c]ommunity concern about the right to and protection of privacy [was] growing as new technologies change the way we interact with business, government, and each other". It invited comment about whether Australia should introduce a statutory cause of action for privacy and, if so, what elements a statutory cause of action might include.[35]

81 It is not clear whether the Department of the Prime Minister and Cabinet ever produced an outcome to its Issues Paper.

82 However, unabashed, in June 2013 the Commonwealth Attorney-General referred to the Australian Law Reform Commission the issue of prevention of and remedies for serious invasions of privacy in the digital era. The first matter the ALRC was asked to address was "innovative ways in which law may reduce serious invasions of privacy in the digital era." It produced an Issues Paper in October 2013 which framed the inquiry it was asked to explore as arising in the following circumstances:

> "[5] The ubiquitous commercial and personal use of digital and affordable mobile technology, across all social and economic strata of society, has been world changing. New technologies allow unprecedented levels of surveillance and tracking of the activities of individuals, of recording and communication of personal information, and of intrusion into physical space. Both aspects of personal privacy that law reform commissions have previously investigated- unauthorised use of personal information and intrusion on personal privacy or seclusion – are significantly affected by the digital era and the capacities that digital technology provides."[36]

83 As ALRC IP 43 notes (at [6]), its work "builds on four other inquiries into privacy law or related issues conducted in Australia since 2006, three of which recommended the enactment of a statutory cause of action".[37]

84 The ALRC has identified the following gaps in Australian privacy law:

- "The Privacy Act and state and territory equivalents deal only with information privacy and not with intrusions into personal privacy.

- The Privacy Act provides for only limited civil redress to individuals who are affected by a breach of the APPs.

- There are a number of organisations that are exempt from the application of the regulatory regime of existing privacy legislation, such as many businesses with an annual turnover of less than $3 million.

- Legislation dealing with surveillance in general, and with workplace surveillance, is not uniform throughout Australia.

- There is no tort or civil action for harassment, nor is there sufficient deterrence against 'cyber-harassment' in Australian law, compared with overseas jurisdictions.

- The tort actions of trespass to the person, trespass to land and nuisance do not provide protection from intrusion into a person's private activities in many situations.

- Legislation and common law protection against aerial and other surveillance does not reflect advances in technology that provide a capacity for new types of invasion into personal privacy.

- Tort law does not provide a remedy for intentional infliction of emotional distress which does not amount to psychiatric illness.

- While the equitable action for breach of confidence can provide effective legal protection against the disclosure of private information, it is less effective after a wrongful disclosure because it is unclear or uncertain whether a plaintiff may recover compensation for emotional distress.

- There is uncertainty, or at least some debate, as to the relevant principles to be applied when a court is considering whether to grant an injunction to restrain the publication of true, private information.

- There is no clear legislative statement protecting freedom of speech, or explicitly requiring it or other matters of public interests to be balanced with the protection of privacy, when the court is considering the grant of an injunction to restrain publication of information or some other alleged invasion of privacy."[38]

85 The ALRC's inquiry continues. It was due to publish a discussion paper at the end of February however if it has, it has not when I last looked a

couple of days ago appeared on its website. It is due to report finally in June. Watch that space.

86 Will anything happen if the ALRC yet again recommends a statutory cause of action for invasion of privacy? There appears to be such a push-back against a statutory cause of action for privacy that governments have not acted. Others, though apparently prepared to accept there ought to be a statutory cause of action for invasion of privacy in Australian law, are only prepared to act on the proviso that its introduction was part of a uniform law exercise.[39] That is a sensible stance having regard to the fact that digital information knows no boundaries.

The European scene

87 I have already referred to the European Union's concern about privacy matters. Let me return to that, albeit briefly.

88 The concept of a "right to be forgotten" was proposed by the European Commission in its 2012 communication on "*Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century*".[40] Partly inspired by figures which suggest that 72% of European internet users were worried they give away too much personal data online and that they did not have complete control over their data, and in an effort to regain that trust, the Commission proposed a "right to be forgotten". This reform of the EU's data protection rules would introduce:

> - **A right to be forgotten**: When you no longer want your data to be processed and there are no legitimate grounds for retaining it, the data will be deleted. This is about empowering individuals, not about erasing past events or restricting freedom of the press (see separate section on this).
>
> - **Easier access to your own data**: A right to data portability will make it easier for you to transfer your personal data between service providers.
>
> - **Allowing you to decide how your data is used**: When your consent is required to process your data, you must be asked to give it explicitly. It cannot be assumed. Saying nothing is not the same thing as saying yes. Businesses and organisations will also

need to inform you without undue delay about data breaches that could adversely affect you.

- **The right to know when your data has been hacked**: for example, companies and organisations must notify the national supervisory authority of serious data breaches as soon as possible (if feasible within 24 hours) so that users can take appropriate measures.

- **Data protection first, not an afterthought**: 'Privacy by design' and 'privacy by default' will also become essential principles in EU data protection rules – this means that data protection safeguards should be built into products and services from the earliest stage of development, and that privacy-friendly default settings should be the norm – for example on social networks or mobile apps.[41]

89 It appears these proposals had not been implemented by the time Vice-President Reding spoke in January this year in favour of a new data protection compact for Europe.

90 Some of these concepts find reflection in the APPs. APP 11.2, for example, in substance requires an APP entity which no longer needs personal information it holds about an individual to take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

Conclusion

91 In *Douglas v Hello! Ltd* [2001] QB 967 (at [110] – [111]), Sedley LJ explained the courts' reluctance to articulate … "a discrete principle of [privacy] law" as "resid[ing] in the common law's perennial need (for the best of reasons, that of legal certainty) to appear not to be doing anything for the first time".

92 As can be seen from this paper, Australian law might be said to be a long way from even suggesting it might do something "for the first time" in the area of privacy. In some respects the courts' silence in this area lies in the absence of suitable fact scenarios which would enable the issues to be confronted head-on. There does not, so far as I am aware, appear to have been a case in Australia which gave the High Court the opportunity to

re-examine the issue of privacy in the digital context, much less from an individual as opposed to a business perspective.

93 Does the failure to develop a "discrete principle of [privacy] law" really matter? Two answers may be given.

94 The first is that while, like "English law [Australian law] has so far been unwilling, perhaps unable, to formulate any such high-level principle [as 'invasion of privacy'], [t]here are a number of common law and statutory remedies of which it may be said that one at least of the underlying values they protect is a right of privacy".[42] As I have said, *Lenah* seemed to leave the door open for further debate – though there appears to be some chance that the legislature may finally move before the courts do.

95 Secondly, as Gummow and Hayne JJ observed in *Lenah* (at [119]):

> "…Privacy law in the United States delivers far less than it promises, because it resolves virtually all these conflicts in favour of information, candour, and free speech. The sweeping language of privacy law serves largely to mask the fact that the law provides almost no protection against privacy-invading disclosures."

96 This appears to be borne out by an observation in *Vidal-Hall*, by Tugendhat J (at [45]) that the issues which concerned the claimants in that case were dealt with in the USA by regulatory authorities (I presume proceeding under statute):

> "…[F]ollowing the discovery of how Google Inc had been collecting the information from Safari browsers in the Relevant Period, Google Inc has faced regulatory sanctions in the USA. In August 2012 it agreed to pay a civil penalty of US$22.5 million to settle charges brought by the United States Federal Trade Commission ("FTC") that it misrepresented to certain users of the Safari browser that it would not place tracking cookies or serve targeted advertisements to those users. Further, on 11 November 2013 it agreed to pay US$17 million to settle US state consumer-based actions brought against it by United States attorneys general representing 37 US states and the District of Columbia. In addition, the Defendant was required to give a number of undertakings governing its future conduct in its dealings with users in the USA."

97 In the meantime, practitioners should be sure their business clients are in a position to comply with the APPs and that their individual clients are aware of their rights under them.

---

[1] I acknowledge the invaluable assistance of my legal researcher, Shanaka Jayasuriya, in the preparation of this address. This address also builds on an earlier paper I gave in 2009, *An Australian Perspective on Privacy Law Developments*, Media Law Resource Centre Conference, London, 30 September 2009 in the preparation for which I was assisted by my then legal researcher, Alice Lam.

[2] http://www.idc.com/about/about.jsp accessed 7 March 2014

[3] ZB is the acronym for "zettabyte" which is a unit of digital information storage used to denote the size of data. It is equivalent to 1,024 exabytes or 1,000,000,000,000,000,000,000 bytes: http://www.techopedia.com/definition/1048/zettabyte-zb accessed 7 March 2014.

[4] http://sites.amd.com/us/Documents/IDC_AMD_Big_Data_Whitepaper.pdf accessed 7 March 2014

http://www.dlapiper.com/files/Publication/2c029f33-f622-4855-97c4-99f6e615cdf8/Presentation/PublicationAttachment/804e7057-fb76-4899-8fad-9ab1291e2939/DLA1252%20-%20Big%20Data%20Privacy%20Update_OneColumn.pdf

[6] Data Protection Day 2014: Full Speed on EU Data Protection Reform, European Commission - MEMO/14/60 27/01/2014 European Commission Press Release Brussels, 28 January 2014 http://europa.eu/rapid/press-release_MEMO-14-60_en.htm accessed 7 March 2014.

[7] http://www.theguardian.com/technology/2012/apr/22/big-data-privacy-information-currency

[8] Data Mining: What is Data Mining? http://www.anderson.ucla.edu/faculty/jason.frand/teacher/technologies/palace/datamining.htm accessed 8 March 2014

[9] The Working Party on the protection of individuals with regard to the processing of personal data ("the Article 29 Working Party"), an independent European advisory body on data protection and privacy set up under Article 29 of Directive 95/46/EC (at p17, cited *Vidal-Hall* (at [90])

[10] Data Mining: What is Data Mining?, *supra*.

[11] An Inquiry into the Culture, Practices and Ethics of the Press - Executive Summary at [1] ("Leveson Executive Summary") http://webarchive.nationalarchives.gov.uk/20140122145147/http://www.official-documents.gov.uk/document/hc1213/hc07/0779/0779.pdf accessed 8 March 2014

[12] Leveson Executive Summary at ([36]).

[13] Australian Law Reform Commission, "*Serious Invasions of Privacy in the Digital Era*", IP 43 ("ALRC IP 43") at [24].

[14] *Australian Broadcasting Corporation v Lenah Game* Meats [2001] HCA 63; (2001) 208 CLR 199 ("*Lenah*")

15 ALRC IP43 (at [22])

16 Warren and Brandeis, "The Right to Privacy" (1890) 4 *Harvard Law Review* 193 (at 195, 196, 205 – 206).

17 Judge Cooley had coined the expression, the "right to be let alone" in his work on *Torts* (2nd ed., 1888, at 29).

18 Warren and Brandeis, supra, (at 195, 196).

19 Warren and Brandeis, supra, (at 214).

20 Warren and Brandeis, supra, (at 218).

21 Dorothy J. Glancy, "*The Invention of the Right to Privacy*", Arizona Law Review, v.21, n.1, pp.1-39 (1979), p.1

22 William L Prosser, "*Privacy*" (1960) 48 *California Law Review* 383 (at 389)

23 See now *Restatement of the Law*, 2nd, Torts 1977 (US) - sections 652B-652D

24 *Australian Broadcasting Corporation v Lenah Game* Meats [2001] HCA 63; (2001) 208 CLR 199 ("*Lenah Game Meats*") (at [323]) per Callinan J.

25 *Campbell v MGN Ltd* [2004] UKHL 22; [2004] 2 AC 457 ("*Campbell*") (at [11]) per Lord Nicholls of Birkenhead referring to *Wainwright v Home Office* [2003] UKHL 53; [2004] 2 AC 406 ("*Wainright*").

26 Ibid.

27 *Wainwright* (at [18]) per Lord Hoffmann

28 Ibid

29 See note 25 above

30 See Australian Law Reform Commission, *Unfair Publication: Defamation and Privacy*, Report No 11 (1979), (at 112-116 [215]-[222]); Australian Law Reform Commission, *Privacy*, Report No 22 (1983), vol 2, (at 21 [1076]): *Lenah Game Meats* (at [186]) per Kirby J, footnote 362. According to IP 43, the 1983 ALRC Report led to the enactment of the *Privacy Act 1988* (Cth).

31 See *Lenah Game Meats* (at [186]) per Kirby J. The ALRC proposed that specific legislation should be enacted which defined the values to be protected, the circumstances of the protection and the defences that would be applicable

32 *Lenah Game Meats* (at [83]) per Gummow and Hayne JJ.

33 *Lenah*, (at [132]) per Gummow and Hayne JJ.

34 Privacy Amendment Bill, Second reading speech Commonwealth of Australia, House of Representatives, *Parliamentary Debates* (Hansard), 23 May 2012 at 5210

35 *A Commonwealth Statutory Cause of Action for Serious Invasion of Privac*y, September 2011, Department of the Prime Minister and Cabinet Issues Paper.

[36] ALRC IP 43.

[37] In addition to those referred to above (at footnotes 13 and 35], there was also the Australian Law Reform Commission report, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008); NSW Law Reform Commission, *Invasion of Privacy*, Report No 120 (2009); Victorian Law Reform Commission (VLRC) *Surveillance in Public Places* (Report No 18) (2010).

[38] ALRC IP 43 at [162]

[39] New South Wales, Law Reform Commission, *Invasion of Privacy*, Report 120 (2009).

[40] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf accessed 2 March 2014

[41] Data Protection Day 2014: Full Speed on EU Data Protection Reform MEMO/14/60 http://europa.eu/rapid/press-release_MEMO-14-60_en.htm accessed 2 March 2014.

[42] *Wainwright* (at [18]) per Lord Hoffmann, a theme to which his Lordship returned in *Campbell* (at [43]); *Lenah* (at [123]) per Gummow and Hayne JJ.