1. Introduction

Contents

This Inquiry

1.1 This Inquiry comes at a time of continuing and rapid advances in technology with increasing capacities to affect the privacy of individuals. Many of these technological advances are beneficial to society and are valued by the individuals and organisations that use them or who benefit from their use. However, these technologies also raise concerns about privacy that might once have been the stuff of science fiction but are now based on reality.

1.2 The challenge for lawmakers is how to ensure that the law remains relevant, appropriate and workable in the light of technological advances. By the 1990s technology had already taken a monumental leap with the development and uptake of the internet and the worldwide web and with advances in digital technology.

1.3 Over the last 20 years, governmental, commercial and personal use of digital technology has become universal. Data-mining methods, search engines and data analytics have revolutionised the processing, recognition, communication, acquisition and aggregation of knowledge and information. Mobile technologies and devices have become increasingly affordable to all social and economic strata of society. Social media have transformed interpersonal communications. Media convergence has made today's media a different phenomenon from even its 1990 counterparts.

1.4 The scope of this Inquiry is not confined to invasions of privacy brought about by digital technology. Significant gaps in data protection regulation, deficiencies or inconsistencies in criminal surveillance or harassment laws, and gaps in the existing common law protection against physical invasions of an individual's privacy also underpin the need for a review of the existing law.

1.5 The divergence in the recommendations of previous inquiries into privacy law, significant developments in other jurisdictions, concerns expressed in the community, continuing gaps in Australian common law and statute law protecting privacy, and new

problems raised by the use of rapidly developing technologies[1] all require detailed consideration by the ALRC in this Inquiry.

1.6 This document commences the second stage in the consultation process in this Inquiry into serious invasions of privacy. The first stage included the release of the Issues Paper, *Serious Invasions of Privacy in the Digital Era* (ALRC IP 43, 2013), in response to which the ALRC received many valuable submissions.[2] The Final Report will be provided to the Attorney-General by the end of June 2014.

How to make a submission

1.7 With the release of this Discussion Paper, the ALRC invites individuals and organisations to make a submission, particularly in response to the specific proposals and questions, but also to any of the background material and analysis.

1.8 There is no specified format for submissions, although the questions and proposals may provide useful guidance. Submissions may be made in writing, by email or using the ALRC's online submission form. Submissions made using the online submission form are preferred.

1.9 Generally, submissions will be published on the ALRC website, unless marked confidential. Confidential submissions may still be the subject of a request for access under the *Freedom of Information Act 1982* (Cth). In the absence of a clear indication that a submission is intended to be confidential, the ALRC will treat the submission as public. The ALRC does not publish anonymous submissions.

> Submissions using the ALRC's online submission form can be made at: <www.alrc.gov.au/content/privacy-subs-DP80>.
>
> In order to ensure consideration for use in the Final Report, submissions must reach the ALRC by **Monday 12 May 2014**.

The Terms of Reference

1.10 The Terms of Reference set out and limit the scope of the ALRC's Inquiry. The ALRC is asked to make recommendations on the detailed legal design of a statutory civil cause of action for serious invasions of privacy. The ALRC is also asked to make recommendations about other legal remedies and innovative ways in which the law could prevent or redress serious invasions of privacy. This latter task has required the ALRC to consider how a range of existing common law causes of action and remedies

---

1 M Paterson notes that 'Surveillance in public places has assumed additional importance in the light of technological developments that have taken place since the publication of the VLRC's report in 2010', citing, for example, increased availability of face and number plate recognition and radio frequency identification technologies: M Paterson, *Submission 60*.

2 Both the Issues Paper and this Discussion Paper may be downloaded free of charge from the ALRC website, <www.alrc.gxjov.au>. Hard copies may be obtained on request by contacting the ALRC on (02) 8238 6333. Public submissions are also published on the ALRC website.

and statutory provisions might be strengthened or amended, as well as considering proposals for new ways in which the law could prevent or redress invasions of privacy.

1.11 The Terms of Reference also require the ALRC to make recommendations which recognise the necessity to balance the value of privacy with other fundamental values—including freedom of expression and open justice. The Discussion Paper addresses this issue at several stages, both in relation to the elements of a statutory cause of action and in relation to existing legal remedies[3] and elsewhere.

Emerging threats to privacy

1.12 Particular attention has been directed recently to the rapidly expanded technological capacity of organisations not only to collect, store and use personal information, but also to track the physical location of individuals, to keep the activities of individuals under surveillance, to collect and use information posted on social media, to intercept and interpret the details of telecommunications and emails, and to aggregate, analyse and sell data from many sources.

1.13 Organisations that may collect and process personal information include:

- national and foreign security organisations;
- government agencies, such as education or health entities or local councils;
- law enforcement agencies;
- media entities;
- financial institutions and credit reporting agencies;
- national and international commercial entities;
- social media platforms;
- retail, marketing and behavioural advertising companies; and
- civilian activist groups.

1.14 Corporate or governmental activities involving the processing of personal information are governed by a range of common law obligations or statutes or regulatory schemes concerned with the collection, storage or dissemination of data or with related matters such as the protection of intellectual, real and personal property, financial interests and reputation.

1.15 Data processing by commercial, government and non-government organisations may often be necessary, appropriate and lawful; carried out with relevant consents or authority or specifically authorised by statute; justified in the public interest; or within the terms and conditions specified by the relevant entity for the provision of a service. Most corporations realise the importance of taking privacy concerns seriously: quite apart from legal reasons, there are important reputational and business consequences of

3 See Ch 12.

data breaches. Many of the organisations described above belong to industry associations which endorse the importance of privacy protection.

1.16 Nonetheless, breaches of privacy do occur as a result of the activities of these organisations for a range of reasons. Some breaches of a person's privacy might be unavoidable; others might come about due to systemic weaknesses in a system of data protection, or through incompetence or lack of care. Some may be caused by deliberate and unpredictable activities of unauthorised third parties, intent on breaking into a data system. Some activities may be outside, or exempt from any existing regulation or law. Some activities may amount to an indefensible, unlawful and deliberate invasion of the privacy of an individual.

1.17 Modern privacy concerns are not however limited to the use of personal information by organisations. Many disputes about invasions of privacy are between individuals. Many of the cases in other jurisdictions involve the conduct of individuals. The ALRC has received submissions from individuals and representative groups concerned about:

- people installing surveillance cameras which can record their neighbour's activities;
- surveillance cameras installed by activists trespassing onto private property and the subsequent posting of the footage on websites; and
- harmful, invasive and distressing disclosure of personal information and images by an individual's former partner.

Previous inquiries and international developments

1.18 This Inquiry builds on four other recent inquiries into privacy law or related issues conducted in Australia, three of which recommended the enactment of a statutory cause of action.[4]

1.19 The ALRC's report, *For Your Information: Privacy Law and Practice* (ALRC Report 108, 2008) focused on data protection: information collection, access and use. The ALRC recommended that Commonwealth legislation should provide for a statutory cause of action for serious invasion of privacy.[5]

1.20 In 2009, the New South Wales Law Reform Commission (NSWLRC) recommended that a general cause of action for invasion of privacy was required to

---

4 Privacy was also the subject of earlier reports by the ALRC. In 1979, the ALRC recommended that a person be allowed to sue for damages or an injunction if 'sensitive private facts' were published in circumstances that were likely to cause distress, annoyance or embarrassment to a person in the position of the relevant individual: ALRC, *Unfair Publication: Defamation and Privacy*, Report No 11 (1979). In 1983, the ALRC released a report concentrating on information privacy, and the need to implement the Organisation for Economic Co-Operation and Development, *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, 1983: ALRC, *Privacy*, Report No 22 (1983). This resulted in the enactment of the *Privacy Act 1988* (Cth).

5 ALRC, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008) Rec 74–1.

provide a 'basis for the ongoing development of the law of privacy in a climate of dynamic societal and technological change'.[6]

1.21 In 2010, the Victorian Law Reform Commission (VLRC) issued the report, *Surveillance in Public Places*, which followed a decade-long inquiry into workplace privacy and privacy in public places.[7]

1.22 In September 2011, the Department of the Prime Minister and Cabinet (DPM&C) released an Issues Paper on a statutory cause of action for invasion of privacy,[8] prompted by a number of 'high profile privacy breaches' in Australia and overseas.[9]

1.23 In addition to a continuing debate in Australia on the desirability of a statutory cause of action, there have been important developments in privacy protection in other countries. Privacy torts have been well-established in the United States for many decades, although the protection they provide is limited by the constitutional protection of free speech in the First Amendment of the US Constitution. Some states, such as California, have also introduced a statutory tort of invasion of privacy.[10]

1.24 The United Kingdom has developed extensive legal protection of privacy by extending the equitable action for breach of confidence, under the influence of the *Human Rights Act 1998* (UK).[11] This Act requires the courts to give effect to the protection of rights and freedoms set out in arts 8 and 10 of the *European Covenant on Human Rights.*

1.25 The Canadian provinces of British Columbia,[12] Manitoba,[13] Newfoundland and Labrador,[14] Quebec[15] and Saskatchewan[16] have enacted statutory torts for invasion of privacy, and the Ontario Court of Appeal has also recognised common law protection.[17] New Zealand courts have recently recognised common law torts of misuse of private information[18] and of intrusion.[19]

1.26 The state of development of a country's common law protection of privacy has a significant impact on the question of whether there is a need to legislate for a cause of action. Committees in both the United Kingdom and New Zealand have recommended

---

6 NSW Law Reform Commission, *Invasion of Privacy*, Report No 120 (2009) [4.14].
7 Victorian Law Reform Commission, *Surveillance in Public Places*, Report No 18 (2010).
8 'A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy' (Issues Paper, Department of the Prime Minister and Cabinet, 2011).
9 This presumably referred to the widespread phone hacking by journalists and their sources that led to the Leveson Inquiry in the United Kingdom: Lord Justice Leveson, *An Inquiry into the Culture, Practices and Ethics of the Press*, House of Commons Paper 779 (2012).
10 *California Civil Code* § 1708.8.
11 *Campbell v MGN Ltd* [2004] 2 AC 457. See Ch 12.
12 *Privacy Act*, RSBC 1996, c 373.
13 *Privacy Act*, RSM 1987, c P125.
14 *Privacy Act*, RSNL 1990, c P-22.
15 *Civil Code of Quebec*, SQ 1991, c 64 ss 3, 35–37.
16 *Privacy Act*, RSS 1978, c P-24.
17 *Jones v Tsige* (2012) 108 OR (3rd) 241.
18 *Hosking v Runting* (2005) 1 NZLR 1.
19 *C v Holland* [2012] 3 NZLR 672 (24 August 2012).

against the introduction of a statutory cause of action, in view of the common law developments in those two countries.[20]

1.27 In contrast, a common law tort for invasion of privacy has not yet developed in Australia, despite the High Court leaving open the possibility of such a development, in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd*.[21] While a tort of invasion of privacy has been recognised by two lower court decisions,[22] no appellate court has confirmed the existence of this tort. The general consensus is that the likely direction of the future development of the common law is uncertain.[23]

Should a new cause of action be enacted?

1.28 The ALRC considers that the question of whether a statutory cause of action for serious invasion of privacy would be beneficial to the Australian community is best answered after considering:

- the existing legal protections for privacy;
- the gaps in that legal protection identified;
- the precise elements of the proposed cause of action; and
- any alternative ways in which the unacceptable gaps in the law might be filled.

1.29 Only a very few stakeholders who made submissions to the Inquiry told the ALRC that the law did not need to be changed at all, and that there were no gaps in the legal protection of privacy in Australia.[24] Those who opposed the introduction of a new cause of action recognised the gaps in the law, but submitted that it would be preferable to fill those gaps in other ways.[25] Many other stakeholders expressed their support for a statutory cause of action. Both stakeholders who supported and those who opposed the introduction of a new cause of action made submissions as to the desirable elements of any such action.

1.30 The cause of action proposed in this Discussion Paper is more precise than similar privacy actions recommended in other law reform reports, and in some respects more narrow. The ALRC believes that precision is important so that stakeholder groups, individuals and lawmakers can reach a more informed view on the potential interpretation and application of the proposed action, on the extent of protection it may provide to potential claimants, and on the impact it may have on those who would face potential liability. Only when these assessments are made can there be an informed

---

20 Joint Committee on Privacy and Injunctions, *Privacy and Injunctions*, House of Lords Paper No 273, House of Commons Paper No 1443, Session 2010–12 (2012); New Zealand Law Commission, *Invasion of Privacy: Penalties and Remedies: Review of the Law of Privacy Stage 3*, Report No 113 (2010).

21 *Australian Broadcasting Commission v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199.

22 *Grosse v Purvis* [2003] QDC 151 (16 June 2003); *Doe v Australian Broadcasting Corporation* [2007] VCC 281. Both cases were settled before appeals by the respective defendants were heard.

23 The case law on the issue since *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* is discussed in Ch 3.

24 Free TV, *Submission 55*; The Newspaper Works, *Submission 50*.

25 SBS, *Submission 59*; AIMIA Digital Policy Group, *Submission 56*; News Corp Australia, *Submission 34*.

debate on the relative desirability of the proposed statutory cause of action or other alternatives.

1.31 Privacy law must recognise other values and interests, such as freedom of expression. This is reflected in the design of the tort proposed in this Discussion Paper. While this may mean that one interest is not as protected or as unconstrained to the extent some advocates would prefer, the ALRC considers that the law may be able to find a middle ground where a balance can be reached and a degree of useful protection can be enacted.

1.32 The statutory cause of action is thus directed at serious invasions of privacy committed intentionally or recklessly with no countervailing justification or defence. If the statute provides remedies for such invasive conduct, Australia will have made an important and clear step in providing greater protection for privacy than is currently available. It will give Australians the privacy protections enjoyed by those in other countries, including the UK, New Zealand and Canada.

1.33 The statutory cause of action is not, however, the only way that greater protection could be achieved by statutory reform. This Discussion Paper, in Part 3, suggests other measures that should be considered to improve the protection in Australia of people's privacy in the digital age, some in addition to and some as an alternative to a new statutory cause of action.