PRIVACY PROTECTION IN AUSTRALIA: A PUBLIC AFFAIR

I INTRODUCTION

The potential misuse of emerging Big Data technologies poses a significant risk to the privacy of personal information. This concern is legitimised by instances of misuse which have already transpired.[1] Notwithstanding, Australian law does not recognise the right to privacy. The right does not exist in legislation and the High Court of Australia has strongly resisted the recognition of the right to privacy in Australian common law (*ABC v Lenah Game Meats Pty Ltd* [2001]). A contrary position is adopted by the European Union and by other common law jurisdictions including the United Kingdom (*Human Rights Act 1998* (UK)).

This paper will discuss the existing privacy protection framework in Australia and will conclude that reform is required in order to guard against intrusions into one's private affairs and protect individuals from the non-consensual collection, use and disclosure of their private information by commercial and public entities.

II DEFINITIONS

A '*Big Data'*

The term 'Big Data' has no exhaustive definition, rather it broadly relates to 'the way in which information is processed and used to inform decision-making' (Paterson & McDonagh 2018, p. 1). Big Data enables the analysis (by artificial intelligence applications or otherwise) of voluminous troves of online personal information to 'seek out correlations' (Paterson & McDonagh 2018, p. 4). Consequently, entities are capable of accurately predicting future

[1] See, for example, the Cambridge Analytica scandal (Schneble et al. 2018) and more recently the exposure in 2020 of profile data of approximately 235 million TikTok, Instagram and YouTube users (Bischoff 2020).

behaviour by identifying and analysing these correlations. While Big Data analysis undoubtedly has beneficial use cases, it is the potential for its misuse which warrants reform of Australia's privacy protection framework.

B *'Personal Information'*

'Big Data' includes personal information. In this paper, 'personal information' takes on its corresponding definition in the *Privacy Act 1988* ('the Act'): 'information or an opinion about an identified individual, or an individual who is reasonably identifiable' (*Privacy Act 1988*, s 6).

C *'Invasion of privacy'*

While debate exists as to how invasions of privacy ought to be defined (*ABC v Lenah Game Meats Pty Ltd* [2001]), this paper shall adopt the approach taken by the Australian Law Reform Commission ('ALRC') (2014, p. 73) which suggests there are 2 categories of invasion: misuse of personal information, and intrusion upon seclusion (both of which are defined below). An 'invasion' or 'breach' of privacy is defined herein as including either case.

D *'Misuse of personal information'*

The 'misuse' of personal information relates to the collection, analysis or disclosure of the information by another individual or entity without the consent of the individual to whom the data relates (*Privacy Act 1988*, sch 1 part 3).

E *'Intrusion upon seclusion'*

'Intrusion upon seclusion' is the unwarranted intrusion into one's 'personal and private moments, even if they occur in a public space' (Vaile, cited in Dombosch 2014, p. 20). The

ALRC (2014, p. 9) provides the example of 'physically intruding into the [person's] physical space or by watching, listening to or recording the [person]'s private activities … or affairs.'

III DEFICIENCIES ASSOCIATED WITH THE EXISTING AUSTRALIAN PRIVACY PROTECTION FRAMEWORK

The collection, use and disclosure of personal information is broadly regulated by the Australian Privacy Principles ('APPs') (*Privacy Act 1988,* sch 1 part 3). If an individual suspects that their information has not been handled in accordance with the APPs (which itself may be difficult to ascertain), a complaint may be made to the Office of the Australian Information Commissioner ('OAIC'), which will then investigate whether or not a contravention of the APPs has occurred (*Privacy Act 1988,* s 36A). Compensation is generally unavailable under the Act, subject to exceptions relating to invasions of privacy by credit reporting bodies (*Privacy Act 1988,* Div 7) or where there are serious and repeated invasions of privacy (although this does not amount to a statutory tort and the meaning of 'serious and repeated' is left open to interpretation) (*Privacy Act 1988,* s13G).

Importantly, the APPs apply only to certain government agencies and to commercial organisations with an annual turnover exceeding $3 million ('APP entities') (*Privacy Act 1988,* s 6). Many small businesses in Australia are therefore not required to comply with the APPs. In the case of an invasion of privacy by such an entity, an individual may therefore be without the ability to seek remedy for any loss or harm suffered as a result.

Further, the APPs do not apply to certain political organisations (including Members of Parliament) when performing acts associated with elections or with the organisations' participation in political process (*Privacy Act 1988,* s 7C). This exemption continues to apply despite recent attempts to utilise personal data in order to influence political outcomes (Schneble et al. 2018).

Finally, the regime of privacy protection afforded by the Act is deficient in that it does not in fact regulate invasions of 'privacy'. The Act affords only 'pseudo-protection' (Vaile, cited in Dombosch 2014, p. 20) and its primary focus is the regulation of the collection, use and disclosure of information by APP entities. The Act therefore does little to ensure a reasonable expectation of privacy from intrusion into one's personal affairs or to set out potential remedies for those who have suffered loss as a result of such intrusion.

To that end, the Act fails to provide adequate remedy for harm resulting from invasions of privacy and from intrusion upon seclusion, which the ALRC considers to be 'materially different than what is regulated by the *Privacy Act*' (Fair, cited in Dombosch 2014, p. 21).

IV A WAY FORWARD: RECOGNISING PRIVACY AS AN ENFORCEABLE CIVIL RIGHT

The introduction of a statutory tort of invasion of privacy would offer protection to individuals for loss or harm resulting from intrusion upon seclusion or misuse of their personal information. This is not a novel idea. It is expressly recommended by the ALRC (2014, p. 19) in its comprehensive 2014 report into privacy law reform. Notably, the ALRC report recommends that serious invasions of privacy by 'intrusion into seclusion or by misuse of private information' should be essential features of the tort. The invasion of privacy 'need not cause actual damage, and 'damages for emotional distress may be awarded' (ALRC 2014, p. 19).

The United Kingdom recognises the right through its ratification of Article 8 of the *European Convention on Human Rights* which must be enforced in its domestic Courts (*Human Rights Act 1998* (UK)). Common law in the United States recognises both the torts of intrusion upon seclusion and general invasion of privacy (ALRC, p. 19).

In those jurisdictions, individuals who suffer loss or harm resulting from serious invasions of privacy are therefore able to claim compensation from the breaching entity to remedy their loss or harm. That is not so in Australia.

Arguments contrary to the introduction of the tort include difficulty in identifying the scope and definition of 'privacy' and when information ought to be treated as private as opposed to public. This problem was described by the High Court in *ABC v Lenah Game Meats Pty Ltd* [2001] HCA 63 (per Gleeson CJ) as 'reason for caution in declaring a new tort … [of privacy]'. The Court further opined that there exists tension between 'interests in privacy and interests in free speech' which warrant a similar exercise of caution.

These arguments are unconvincing in circumstances in which both the right to privacy and the right to free speech are contemporaneously protected by law in both the United Kingdom and the United States. Likewise, if the tort was targeted specifically to against the misuse of personal information intrusion upon seclusion (as the ALRC (2014, p. 73) recommends), difficulties in identifying when a compensable invasion of privacy has occurred would be greatly reduced. The arguments against the introduction of the tort suggested by the Court in this case are outweighed by the rapid development of Big Data technologies and the potential for their misuse.

V CONCLUSION

It has been illustrated that the privacy framework in Australia does not protect individual privacy in the sense of the misuse of one's personal information or intrusion upon seclusion. Its focus remains on regulating the collection, use and disclosure of information by entities subject to the APPs, thus affording insufficient avenues of recourse to individuals aggrieved by invasions of privacy.

Despite the strong recommendations of the ALRC being published in 2014, Australia is yet to recognise the right to privacy and to introduce a statutory tort for invasion of privacy. It remains to be seen whether the recommendation will be adopted by the legislature.

It is paramount that the development of Australia's privacy protection regime matches the rapid pace of the development of Big Data technology and analysis techniques. Australia is otherwise at risk of remaining behind other jurisdictions and leaving its population open to serious intrusions into individual private affairs and the misuse of personal information.

The introduction of a statutory tort of invasion of privacy would embolden the existing regime, afford individuals remedy when wronged by intrusions upon seclusion or misuse of personal information, and enshrine in our domestic legislation what is recognised elsewhere in law as a universal human right.

REFERENCES

ABC v Lenah Game Meats Pty Ltd [2001] HCA 63.

Australian Law Reform Commission 2014, *Serious Invasions of Privacy in the Digital Era*, Australian Law Reform Commission, Sydney.

Bischoff, P 2020, *Social media data broker exposes nearly 235 million profiles scraped from Instagram, TikTok and Youtube*, Comparitech, Comparitech Limited, viewed 8 November 2020, < https://www.comparitech.com/blog/information-security/social-data-leak/>.

Dombosch, G 2014, 'Too much information: the right to privacy in Australia', *Law Society Journal*, vol. 52, no. 4, pp. 20 – 21.

Human Rights Act 1998 (UK).

Paterson, M & McDonagh, M 2018, 'Data protection in an era of big data: The challenges posed by big personal data', *Monash University Law Review*, vol. 44, no. 1, pp. 1 – 31.

Privacy Act 1988 (Cth).

Schneble, C, Elger, B & Shaw, D 2018, 'The Cambridge Analytica affair and Internet-mediated research', *EMBO Reports*, vol. 19, no. 8.