# Privacy and Data Protection in Australia: a Critical overview (extended abstract)

David Watts[1], Pompeu Casanovas[2,3]

[1] La Trobe Law School, La Trobe University, Melbourne, Australia
[2] UAB Institute of Law and Technology, Universitat Autònoma de Barcelona, Spain

**Abstract.** This extended abstract describes the regulation of privacy under Australian laws and policies. In the CRC D2D programme, we will develop a strategy to model legal requirements in a situation that is far from clear. Law enforcement agencies are facing big floods of data to be acquired, stored, assessed and used. We will propose in the final paper a linked data regulatory model to organise and set the legal and policy requirements to model privacy in this unstructured context.

**Keywords:** Australian privacy law, legal requirements, privacy modelling

## 1 Introduction

Australia has a federal system of government that embodies a number of the structural elements of the US Constitutional system but retains a Constitutional monarchy. It consists of a national government (the Commonwealth), six state governments (New South Wales, Victoria, Tasmania, Queensland, South Australia and Western Australia) as well as two Territories (the Australian Capital Territory and the Northern Territory).

Under this system, specific Constitutional powers are conferred on the Commonwealth. Any other powers not specifically conferred on the Commonwealth are retained by the States (and, to a lesser extent, the Territories).

There is no general law right to privacy in Australia. Although Australia is a signatory to the *International Convention on Civil and Political Rights*, the international law right to privacy conferred under Article 17 of the ICCPR has not been enacted into Australia's domestic law. This paper will explore the requirements to model privacy in such a difficult situation, to prevent illegal disclosures and to enhance citizens' constitutional rights.

# 2 Privacy and Information Privacy

## 2.1 Australian legal regime

*Information privacy* in Australia is protected by a combination of Commonwealth, State and Territory legislation each of which include a set of privacy principles that are based on the *Organisation for Economic Co-operation and Development's Guidelines on the Protection of Privacy and Transborder flows of Personal Information* (OECD Principles).

The protection of information privacy in Australia has been referred to as a 'patchwork.' Although all of the relevant laws are based on the OECD Principles, there are significant differences in the way they are applied from jurisdiction to jurisdiction and, in some cases (particularly for health privacy) there are overlaps between Commonwealth and State legislation.

Each of Australia's information privacy regimes are overseen by a Commissioner. Privacy Commissioners are, in broad terms, given responsibility for resolving privacy complaints – typically through a conciliation process. At a Commonwealth level, the Information Commissioner has a role in initiating enforcement proceedings leading to fines of up to $A2,100,000.00.

The *Privacy Act 1988* regulates information privacy in the Commonwealth public sector and the national private sector. It covers personal information and sensitive information (such as health information, ethnicity, sexual preference, trade union membership). It provides a higher level of protection for sensitive information.

There are a number of exemptions, the most important of which is that the private sector privacy protections do not apply to small business operators (unless they collect and handle health information). Small business operators are defined in such a way that it is estimated that this exemption covers 85% of the Australian private sector.

Another important exemption is that employers who collect and handle health information about an employee are not required to comply with privacy obligations in respect of that information.

## 2.2 Territories

A brief overview on the legislation confirms these Australian patchwork-driven regulatory trends. To begin with, there is no public sector information privacy law or protection in South Australia nor in Western Australia.

In New South Wales (NSW) the *Privacy and Personal Information Protection Act 1998* (PIPPA Act) regulates information privacy in the NSW public sector (except health privacy). Health information in NSW is regulated by the *Health Records and Information Privacy Act 2002* (HRIP). The HRIP applies to any public sector or private sector organisation that collects or handles health information in NSW.

In Victoria, the *Privacy and Data Protection Act 2014* regulates information privacy within the Victorian public sector (except health information). The *Health Records Act 2001* regulates information privacy within the Victorian public sector and for any private sector organisation that collects and handles health information.

In Queensland, the *Information Privacy Act 2009* regulates privacy, including health privacy, in the Queensland public sector. The *Personal Information and Protection Act 2004* regulates information privacy in the Tasmanian public sector. The *Information Privacy Act 2014* regulates the collection and handling of personal information (but not health information) by Australian Capital Territory (ACT, Canberra) public sector agencies. The *Health Records (Privacy and Access) Act 1997* regulates the handling of health information by both public and private sector health service providers in the ACT. The *Information Act 2001* regulates information privacy in the Northern Territory. It also covers health information collected and handled in the Northern Territory public sector.

## 3 Key issues

The most significant limitation of Australia's information privacy law is that it does not apply to most of the private sector. Only organisations with a monetary turn-over of $A3,000,000.00 are covered (unless they collect and handle health information or in some instances where credit reporting occurs). Unlike New Zealand, Australia's information privacy laws were not declared as providing 'an adequate level of data protection' under Article 25(2) of the EU Directive 95/46/EC and will not receive a similar declaration under the GDPR.

Sanctions and penalties under Australian information privacy laws are comparatively weak when compared to the European Union, particularly when compared to the sanctions available under the GDPR.

Again, compared to the GDPR, Australia's information privacy laws have not been refreshed by the conferral of additional rights that have become increasingly important for the protection of privacy in the context of Big Data or similar technologies. For example: (i) There is no 'right to be forgotten', (ii) There are no 'data portability' rights, (iii) There is no right to object to the processing of personal information (such as profiling).

Hence, at a Commonwealth level, Australia's information privacy laws have lagged behind European developments and the introduction of new technologies that challenge existing forms of protection. Open Data policies have been adopted by government that have seen 'de-identified' personal information published but with insufficient regard to the inherent limitations of de-identification techniques. Mandatory data breach notification laws that came in to effect in February 2018 do not cover most of the private sector and only require those affected to be notified within a reasonable time. No reform activity has considered the impact of Big Data on Australia's privacy laws.

At the same time, Australia has enacted some of the most far-reaching anti-terrorism and national security laws of any of the western democracies. Amongst other things, these controversial laws have enabled law enforcement and national security agencies to access metadata without warrant and exempt form privacy laws.

At a State and Territory level, public sector privacy protection has been diluted by recent legislative amendments that mandate information sharing between government

agencies and provide for personal information to be made available to government-appointed chief data officers for analysis. The powers of such officers override those of the Privacy Commissioners.

Australia's primary microeconomic reform advisory body, the Productivity Commission, released a report on Data Availability and Use in May 2017. One of its recommendations was the creation of a new consumer data right that would sit alongside privacy rights. The precise nature of such a right is unclear and a government response to this recommendation has not yet been made public.

Australia's anti-trust regulator, the Australian Consumer and Competition Commission, just released an inquiry into Digital Platforms (such as Facebook and Google) in February 26th 2018. The inquiry examines the market power of digital platforms, their implications for content creators, advertisers and consumers, and assesses the effectiveness of existing regulation, and make proposals for change.

## 4 Modelling Privacy in Australia

We intend to develop in this paper the legal and policy requirements to construct privacy models under the Australian law. Tactics, strategies, and indirect strategies to embed protections into the architecture of semi-automated systems will be described and considered. This is the first step to create a benchmark to test the architecture for establishing legal semantic workflows in the context of integrated law enforcement scenarios.

### Acknowledgements

This research is funded by the *Data to Decisions Cooperative Research Centre (D2D CRC)*, Project C, with participation of the Spanish Project *DER2016-78108-P*. Views expressed herein are however not necessarily representative of the views held by the funders.

### References

1. Stumptner, M., Mayer, W., Grossmann, G., Jiu, J., Li, W., De Koker, L., Mendelson, D., Bainbridge, B., Watts, D., Casanovas, P. An Architecture for Establishing Legal Semantic Workflows in the Context of Integrated Law Enforcement, Workshop on Legal Knowledge and the Semantic Web (LK&SW-2016), International Conference on Knowledge Engineering and Knowledge Management, Bologna, Italy, Nov. LNAI, 2018 *arXiv preprint arXiv:1708.06613* (2017).
2. Mayer, W., Casanovas, P., Stumptner, M., de Koker, L., Mendelson, D. "Semantic Workflows in Law Enforcement Investigations and Legal Requirements.", in V. Rodriguez-Doncel, P. Casanovas. J. Gonzalez-Conejero, TERECOM 2017. Proceedings of the 1st Workshop on Technologies for Regulatory Compliance co-located with the 30th International Conference on Legal Knowledge and Information Systems (JURIX 2017) Luxembourg, December 13, 2017. http://ceur-ws.org/Vol-2049/

3.
4. Law and Policy Program. Big Data Technology and National Security - Comparative International Perspectives on Strategy, Policy and Law: Australia (Data to Decisions CRC, 2016).
5. Casanovas, P., De Koker, L., Mendelson, D., Watts, D.. "Regulation of Big Data: Perspectives on strategy, policy, law and privacy." *Health and Technology* 7, 4 (2017): 335-349.
6. Bennett-Moses, L., de Koker, L. Open Secrets: Balancing Operational Secrecy and Transparency in the Collection and Use of Data for National Security and Law Enforcement Agencies, CRC Report. 2017. *Melbourne Law School Review* (forthcoming)
7. Australian Government. Data availability and use. Productivity Commission Inquiry Report, No. 82, 31 March 2017.
8. Australian Government. ACC, Digital Platforms Inquiry Issues Paper, 26 February 2018.
9. Casanovas, P. Cyber Warfare and Organised Crime. A Regulatory Model and Meta-Model for Open Source Intelligence (OSINT). In R. Taddeo and L. Glorioso, Ethics and Policies for Cyber Operations,pp. 139-167: Dordrecht: Springer International Publishing, 2017.
10. Poblet, M. and Plaza, E. (2017). Democracy Models and Civic Technologies: Tensions, Trilemmas, and Trade-offs. *arXiv preprint arXiv:1705.09015*.
11. Watts, D., Bridget Bainbridge, B., de Koker, L., Casanovas, P., Smythe, S. Project B.3 A Governance Framework for the National Criminal Intelligence System (NCIS), Data to Decisions Cooperative Research Centre, La Trobe University, 30 June 2017.
12. Watts, D. Report of the Special Rapporteur on the right to privacy. United Nations. A/72/43103, October 19th 2017.
13. Clark, R. Guidelines for the responsible application of data analytics. *Computer Law & Security Review* 2017 (in press) https://doi.org/10.1016/j.clsr.2017.11.002
14. Rodríguez-Doncel, Víctor, Cristiana Santos, Pompeu Casanovas, and Asunción Gómez-Pérez. "Legal aspects of linked data–The European framework." *Computer Law & Security Review* 32, no. 6 (2016): 799-813.
15. Casanovas, P., Palmirani, M., Peroni, S.,van Engers, T.v., and Vitali. F. "Semantic web for the legal domain: the next step." *Semantic Web* 7, no. 3 (2016): 213-227.
16. Casanovas P, De Koker L, Mendelson D, Watts D. Regulation of Big Data: Perspectives on strategy, policy, law and privacy. *Health and Technology* 2017 Dec 1;7(4):335-49.
17. Casanovas , González-Conejero J, de Koker L. “Legal Compliance by Design (LCbD) and through Design (LCtD): Preliminary Survey”, in V. Rodriguez-Doncel, P. Casanovas. J. Gonzalez-Conejero, TERECOM 2017. Proceedings of the 1st Workshop on Technologies for Regulatory Compliance co-located with the 30th International Conference on Legal Knowledge and Information Systems (JURIX 2017) Luxembourg, December 13, 2017. http://ceur-ws.org/Vol-2049/