A review of information privacy laws and standards for secure digital ecosystems

Memoona J. Anwar
Faculty of Engineering and Information Technology
University of Technology Sydney
Ultimo, NSW 2007, Sydney, Australia
Email: memoona.j.anwar@student.uts.edu.au

Asif Q. Gill
Faculty of Engineering and Information Technology
University of Technology Sydney
Ultimo, NSW 2007, Sydney, Australia
Email: asif.gill@uts.edu.au

Ghassan Beydoun
Faculty of Engineering and Information Technology
University of Technology Sydney
Ultimo, NSW 2007, Sydney, Australia
Email: ghassan.beydoun@uts.edu.au

Abstract

Information privacy is mainly concerned with the protection of personally identifiable information. Information privacy is an arduous task, in particular, in the context of complex adaptive and multi-party heterogeneous digital ecosystems. There is a need to identify and understand the relevant privacy laws and standards for designing the secure digital ecosystems. This paper presents the results of our information privacy research in digital ecosystems through the lens of local and international privacy regulations and standards. A qualitative research method was applied to review a set of identified privacy laws across the four layers of digital ecosystem. The evaluation criteria has been applied to evaluate the applicability and coverage of the selected seven information privacy laws to people, process, information and technology layers of the digital ecosystems. The research results indicate that information privacy is a critical phenomenon; however, it is not adequately addressed in the context of end-to-end digital ecosystems. It is recommended that a multi-layered privacy by design approach is required by reviewing and mapping information privacy laws and standards to design the secure digital ecosystems.

Keywords: Information Privacy, Information Security, Privacy, Regulations, Digital Ecosystems, Cyber Security

1 Introduction

There are growing concerns about the privacy of information or data collected by the governments, private organizations and employers. Privacy includes concerns of collection, data transmission, data storage, access and rights, usage and disclosure of personal information (Moghe 2003). Technology, such as cloud (Gill et al. 2014), has allowed government and commercial entities to collect, use and disclose huge sets of personal identification information (PII) irrespective of the consent of information owners. The information is collected from multiple platforms. When managing multiple platforms, it is important to understand how they will interact to achieve the business goal. This is where digital ecosystems come into picture. A digital ecosystem (DE) is a comprehensive picture of how all digital and social components of an organisation interconnect and interact (Schmidt 2014). Hence, a digital ecosystem is a coordinated network of interacting platform such as business organisations, digital devices and consumers that create value. Common examples of digital ecosystem (DE) are healthcare ecosystem, financial services ecosystem etc. When the information is collected from multiple sources, the owner may not know its usage. Many business entities use this information for commercial gains e.g. email spam, marketing campaigns and cross selling of information or products. There has to be a well-defined check and balance mechanism, which can monitor and control the unwanted use of personal information. For that matter, we need some regulations through which this use or misuse of information can be controlled. The *Australian Constitution* defines a federal system of government according to which, powers are divided among the Commonwealth (national government), six states (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). However, complying with Australian privacy laws is still challenging for private sector organizations.

Many laws have been formulated and amended over a period of time in order to ensure privacy of individuals. The **Privacy Act 1988** regulates information privacy in the Commonwealth public sector and the national private sector in Australia. It covers PII and other sensitive information (such as health information, ethnicity, sexual preference, trade union membership). The Privacy Act (1988) is based on thirteen **Australian Privacy Principles (APPs**), which are applicable to most of the Australian and Norfolk Island government agencies as well as to some private sector organisations. The **Protective Security Policy Framework (PSPF)** provides assistance to Australian Government entities in protecting their people, information and assets, at both domestic and international (PSPF 2016). The Australian Signals Directorate (ASD) provided the Australian Government **Information Security Manual (ISM)[19].** The standard oversees the security of government ICT systems (ISM 2017). It adds to the features of PSPF (Australian Cyber Security Centre (ACSC) 2018). The **NIST Cybersecurity Framework** provides a privacy guide in the form of a policy framework regarding the way private sector organizations in the US can measure and improve their ability for prevention, detection, and responding to cyber-attacks (NIST Framework for Improving Critical Infrastructure Cybersecurity 2018). Most recently, the **Mandatory Data Breach Notifications(MDBN)** laws followed by other laws coming into effect in Australia, to make sure that individual entities in the digital ecosystems, including federal entities, big businesses, small to medium-size enterprises (SMEs), and customers need fulfilling their responsibility in making Australia "cyber secure", according to Senator Bridget McKenzie (2017). Further, recent introduction of the **EU General Data Protection Regulation (GDPR)** is another requirement for the business to consider. The GDPR was aimed to blend data privacy laws across Europe, to guard and authorize all EU nationals' information privacy and to redesign the way organisations across the region interpret and address information privacy. Australians also need to have the assurance of information privacy. Thus, the management and ongoing maintenance of privacy provisions for digital data is very challenging, because of the wide range of interconnected yet often different laws that apply to different types of information and sectors (Holt and Malcic, 2015). Privacy regulators face a mass of challenges as well when dealing with the data that spreads outside legal boundaries in digital ecosystems (Sinha 2018). This draws our attention to the following research challenge.

RQ: What is the scope and relevance of key national and international privacy laws for digital ecosystems?

This paper presents a review and mapping of national and international information privacy laws and standards to inform the secure design of the digital ecosystems. The paper evaluates the relevance and

coverage of seven laws. Further, it recommends that there is a need for a complete end-to-end framework that should address privacy concerns throughout the information life cycle and is embedded in the design of all the layers of the digital ecosystem.

The paper is organized as follows. Firstly, it provides the research background to set the context for this study. Secondly it presents the research method and review criteria. Thirdly, it presents the review and mapping results. Fourthly, it discusses the review results and its implications. Finally, it concludes with key learnings and future research directions.

2 Background

Information privacy in Australia is protected by a combination of Commonwealth, State and Territory legislations, which often includes a collection of privacy principles that are based on the Organisation for Economic Co-operation and Development's Guidelines on the Protection of Privacy and Trans-border flows of Personal Information (OECD 2003). The protection of information privacy in Australia has been referred to as a 'patchwork' (Patchwork NSW 2014). Although, all of the relevant laws are based on the OECD principles, there are substantial dissimilarities in the approach they are applied from industry to industry and, in some cases (particularly for health privacy); there are overlaps between Commonwealth and State legislations. A brief summary (Table 1) on the legislation confirms these Australian patchwork-driven regulatory trends. To begin with, there is no public sector information privacy law or protection neither in South Australia nor in Western Australia (ALRC 2007). 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). The Health Records and Information Privacy Act 2002 (HRIP) regulate health information in NSW. The HRIP applies to any public sector or private sector organisation that collects or handles health information in NSW (Croucher 2011). 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.

Table 1 summarises the Australian privacy laws and their corresponding sectors of applicability. Each of Australia's information privacy regimes are overseen by the Commissioner. Privacy Commissioners are, in broad terms, given responsibility for resolving privacy complaints – typically through a conciliation process.

Industry	Standard/Regulation
Healthcare	Privacy Act (1988) (applicable to private sectors only), Royal Australian College of General Practitioners (RACGP), Computer and Information Security Standards, National Health and Medical Research Council's "The Regulation of Health Information Privacy in Australia"., National Health Act 1953, Healthcare Identifiers Regulations 2010, Healthcare Identifiers Act 2012 (HI Act), My Health Records Rule 2016 , My Health Records Regulation 2012. Mandatory Data Breach Notifications (MDBN) ISO 270001/2, COBIT5
Internet services	Communication Alliance C650:2014 icode, Australian Communications and Media Authority's "Australian Internet Security Initiative" (ACMA, 2015), Telecommunications and Listening Device Amendment Act. ISO 270001/2 and COBIT5
Federal Government	Australian Government Protective Security Framework (PSPF), Privacy Act (1988), Information Security Manual(ISM), Mandatory Data Breach Notifications (MDBN), Australian Government Agencies Privacy Code (1st Jul,2018)
Cross Border Information Sharing	APP 8, Australian Federal Police Act 1979 (Cth), Mutual Assistance in Criminal Matters Act 1987 (Cth), Anti-money Laundering and Counter-terrorism Financing Act 2006 (Cth)

Defence	Crimes Act 1914
Taxation	Australian Privacy Principles (APP), Taxation Administration Act 1953, Income Tax Assessment Act 1936, Superannuation Industry (Supervision) Act 1993, Retirement Savings Accounts Act 1997, Data-matching Program (Assistance and Tax) Act 1990
Education	Unique Student Identifier (USI),
Banking and finance	APRA CPG 235 and PPG 234, relevant subsections of section RG104 of AFSL license obligation (RG104.93 and RG 104.96), Anti-Money Laundering And Counter-Terrorism Financing Act (Cth), Financial Transaction Reports Act (Cth), ISO270001/2 and COBIT5
Human Rights & Social Behaviour	Australian Human Rights Commission Act 1986, Human Rights (Sexual Conduct) Act 1994, ALRC Report 123 (2014), s.15,
Digital Ecosystems	Partial Coverage. No industry specific law
Manufacturing	None, recommended to follow ISO270001/2 and COBIT5
State Government	Mostly states are using PSPF and ISM as baseline
Mining	No particular Law, Recommended to follow ISO270001/2,ISO 27019 and COBIT5
Utilities	No particular Law, Recommended to follow ISO270001/2, ISO27019 and COBIT5
Retailers	No particular Law, Recommended to follow ISO 270001/2, ISO 27019 and COBIT5
Telecommunications	Telecommunications and Listening Device Amendment Act, Australian Communications and Media Authority's "Australian Internet Security Initiative"(ACMA,2015), Telecommunications Act 1997, Telecommunications(interception and access) Act 1979 ISO270001/2 and COBIT5
Small Businesses	Do Not Call Register Act 2006 (Cth) , Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act

Table 1. Summary of Industries and Corresponding Laws

Privacy Act is the primary element of federal legislation regulating privacy in Australia. The Act controls the management of personal information by the Australian Government, the ACT Government and the private sector. It covers personal information and sensitive information e.g. health records. It provides a higher level of protection for sensitive information. There are a number of exceptions, the most vital of which is that the private sector privacy protections do not apply to small business operators (unless they collect and handle health information). Another important exemption is that employers who collect and handle health information about an employee are not bound to comply with privacy compulsions in respect of that information (ALRC 2007).

Other federal legislations also regulate the handling of personal information. For example, the *Freedom of Information Act 1982* (Cth) (FOI Act) provides access rights to each individual to the documents held by government agencies or Ministers, other than exempt documents. The conduct of tax file numbers (TFNs) is controlled by different federal Acts including the *Income Tax Assessment Act 1936* (Cth) and the *Taxation Administration Act 1953* (Cth). The *Data-matching Program (Assistance and Tax) Act 1990* (Cth) regulates data-matching using TFNs. Federal legislation also contains a large number of secrecy provisions that impose duties on public servants not to disclose information that comes to them by virtue of their office(ALRC 2007). Each Australian state and territory controls the administration of personal data. In some states and territories, personal information is regulated by legislative schemes, in others by administrative regimes (ALRC 2008).

After review of the currently applicable information security laws and regulations, it is obvious that Australia has a few common information security laws but is missing some of the industry specific standards. For those missing regulations in Australia, Australian organizations can adopt related international frameworks. For example, Australian Securities and the investment corporation recommends adopting NIST cyber security framework (ASIC 2015). However, with digital ecosystems, there is no specific well-established privacy law that covers end-to-end lifecycle of data, locally as well as internationally. As discussed earlier, there are many privacy laws and regulations to choose from and thus need to be reviewed for digital ecosystems. Nonetheless, a single privacy law usually does not

provide end-to-end (high to low level) privacy as is required by digital ecosystem. In order to ensure privacy of information in digital ecosystem, there should be a complete privacy framework that covers the entire lifecycle of information, starting from its collection to destruction across all the architecture layers (e.g. people, process, information, technology) of the digital ecosystem (Gill 2015).

3 Research Method

This review uses the four layers (e.g. people, process, information, technology) of digital ecosystem in order to evaluate the relevance of selected regulations. The four layers were adapted from the adaptive enterprise architecture modelling by (Gill 2015). We adopted a document based qualitative research method to review a set of key privacy laws across the selected layers of digital ecosystem architecture (Bashir and Gill, 2016). The qualitative approach seems appropriate in the context of this paper as it allowed to review the seven well-known privacy regulations from high to low level, as required and fit in the context of research question in hand. Like other analytical methods in qualitative research, document analysis requires that data be examined and interpreted in order to elicit meaning, gain understanding, and develop empirical knowledge (Bowen 2009). Each regulation is measured against different attributes (Fig 3, Fig 4, Fig 5, Fig 6) of digital ecosystem's layers. The potential source of data for deriving the attributes of each layer; is official documents of mentioned compliance regulations (APP, Privacy Act, ISM, PSPF, MDBN, NIST, PSPF).

The *Privacy Act* and many other legislations (FoI Act, TFNs etc) were enacted before the rise of Big Data and neither adequately addresses the concerns of individuals or provides clarification for business regarding the steps that should be taken to manage the competing interests. There is no straight forward law that provides guidelines in balancing the protection of an individual's privacy against the business desire to use this valuable "new economic asset" that is Big Data (Christie and Saadati, 2013).

This paper reviews the most recent literature published on privacy laws in the context of digital ecosystems. Each layer of DE is further broken down into certain attributes and applicability of chosen laws is checked individually for each attribute. Table 2 summarises the selected laws and review criteria that is used in this study.

BDE Layer	Standard/Regulation						
	APP	Privacy Act(1988)	PSPF	ISM	NIST	MDBN	GDPR
People	How do these regulations and standards support privacy of people related to DE?						
Process	How do these regulations and standards support processes involved to carry out functioning of DE						
Information	How do these regulations and standards ensure privacy of information/data in DE						
Technology	How do these regulations and standards ensure privacy through technology used in DE						

Table 2. Review Criteria

4 Results

This section applies the review criteria mentioned in table 2, and presents the review and detailed mapping of seven well-known privacy regulations. As discussed earlier, the aim of this paper is to review these standards from digital ecosystem's perspective. This paper assembles many of the information security related legal and regulatory requirements of the federal government of Australia.

With so many interconnected devices and huge amount of data at stake, the need for cyber and data security has reached levels seen never before in the history of internet era. The more the data with an organization, the more valuable the organization is for an attacker (Joshi 2017). The generation and exploitation of big data is key element of digital ecosystems (Urbiola 2018). Digital ecosystems can improve the quality of their services by combining and exploiting big data properly. This allows DE to increase customer involvement and make new customers, obtaining yet more information and continuing to improve their worth. However, the application of key privacy principles, together with notice and consent, data collection and retention, as well as use limitation, is dealt with differently in big data domain (OAIC 2016). Other than privacy and spam acts, Australian laws do not currently regulate Big Data (Christie and Saadati, 2013). This paper reviews seven of the most recent privacy laws in Australia with reference to digital ecosystem and evaluates them according to all the layers. Figure 1 shows the collective coverage offered by seven laws under study for four layers of digital ecosystem. We have mapped each law, one by one to the attributes of each layer and turned the flag on if it was applicable to any particular attribute. Ideally, if there was a complete coverage of privacy offered by the laws under discussion; each attribute should have all seven flags on against each law. In the end, the total score of all the flags was taken and percentage was calculated. According to this calculation, people layer seems to have highest applicability from the laws with 28.6 percent whereas technology layer has least controls applicable to it with a percentage of 25.5%. The process and information layer both lie more or less at the same point with 27% and 28% controls. Figure 2 shows what percentage each laws has in each layers. For example, GDPR is applicable to 70% of people layer attributes, 34.6% of process layer attributes, 52% of information layer and 57% of technology layer.

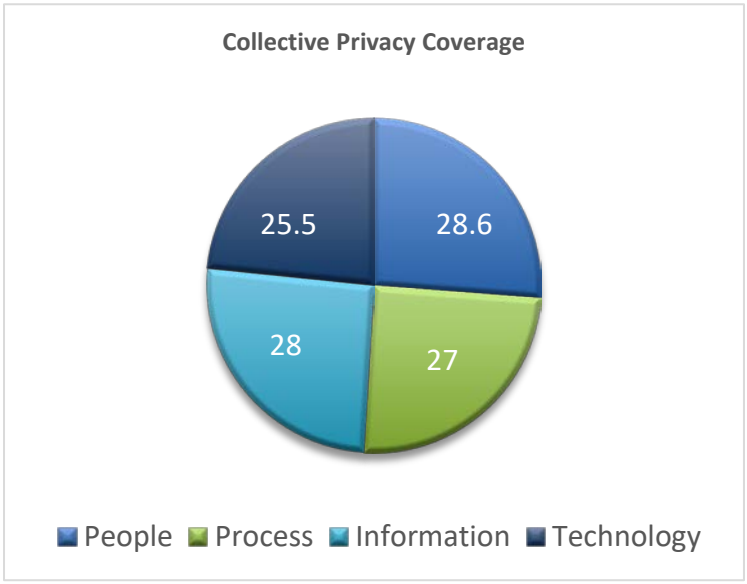

Figure 1: Collective Privacy Coverage

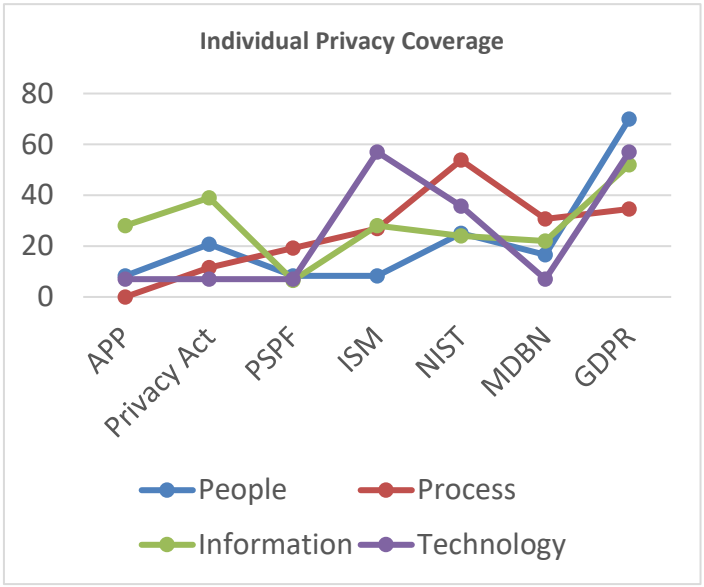

Figure 2: Individual Privacy Coverage

Figure 3, figure 4, figure 5 and figure 6 illustrate the mapping of Australian privacy laws on DE.

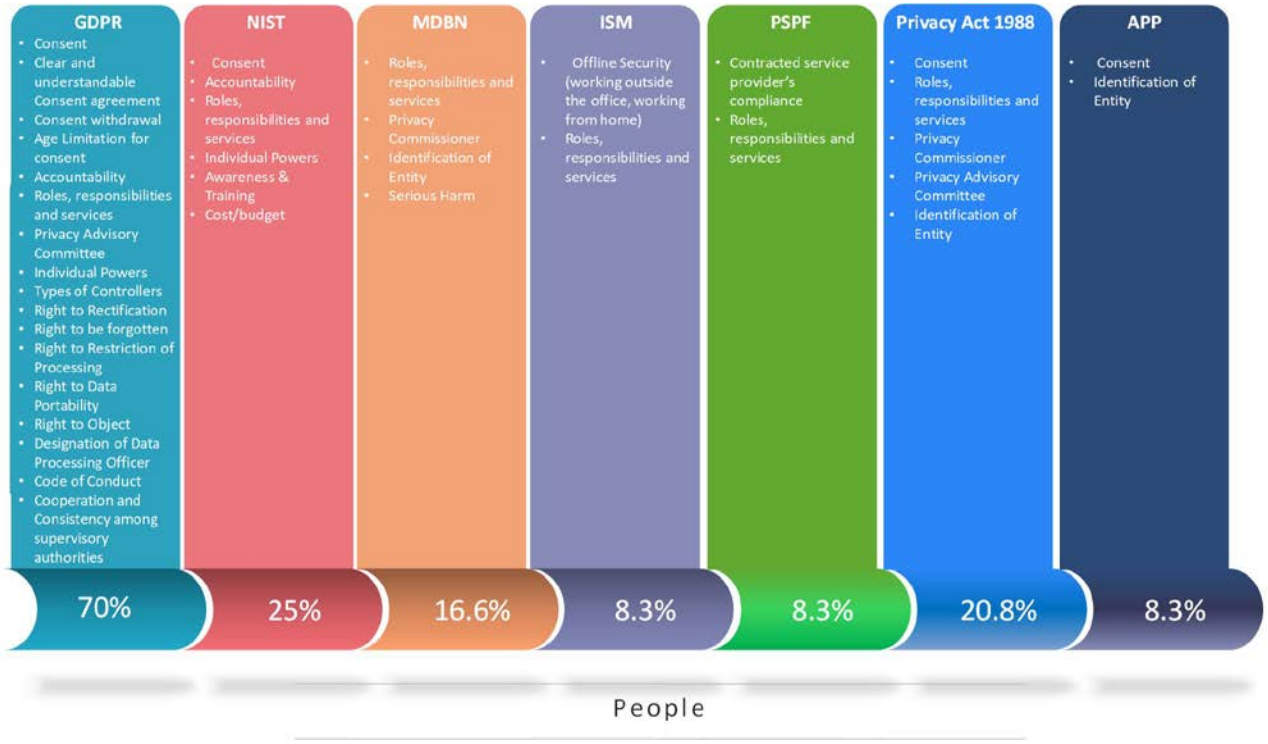

Figure 3: Division of People Layer and Applicability of laws

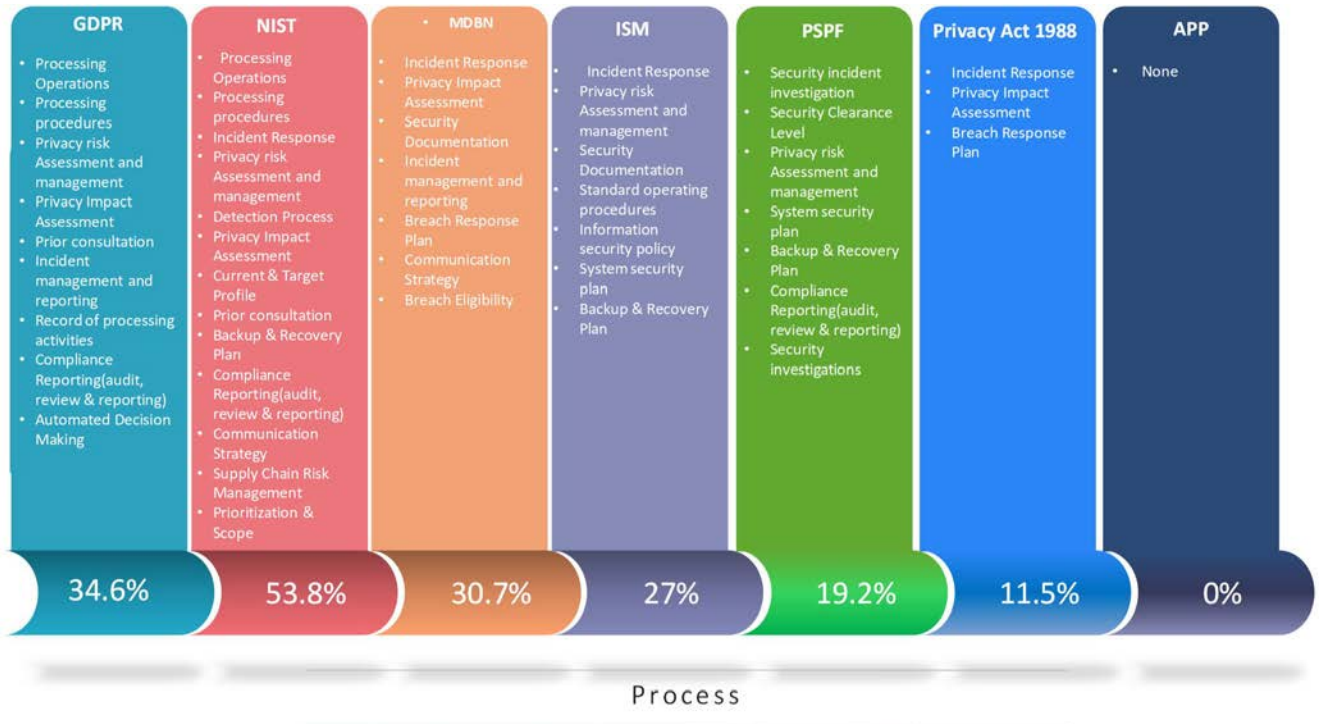

Figure 4: Division of People Layer and Applicability of laws

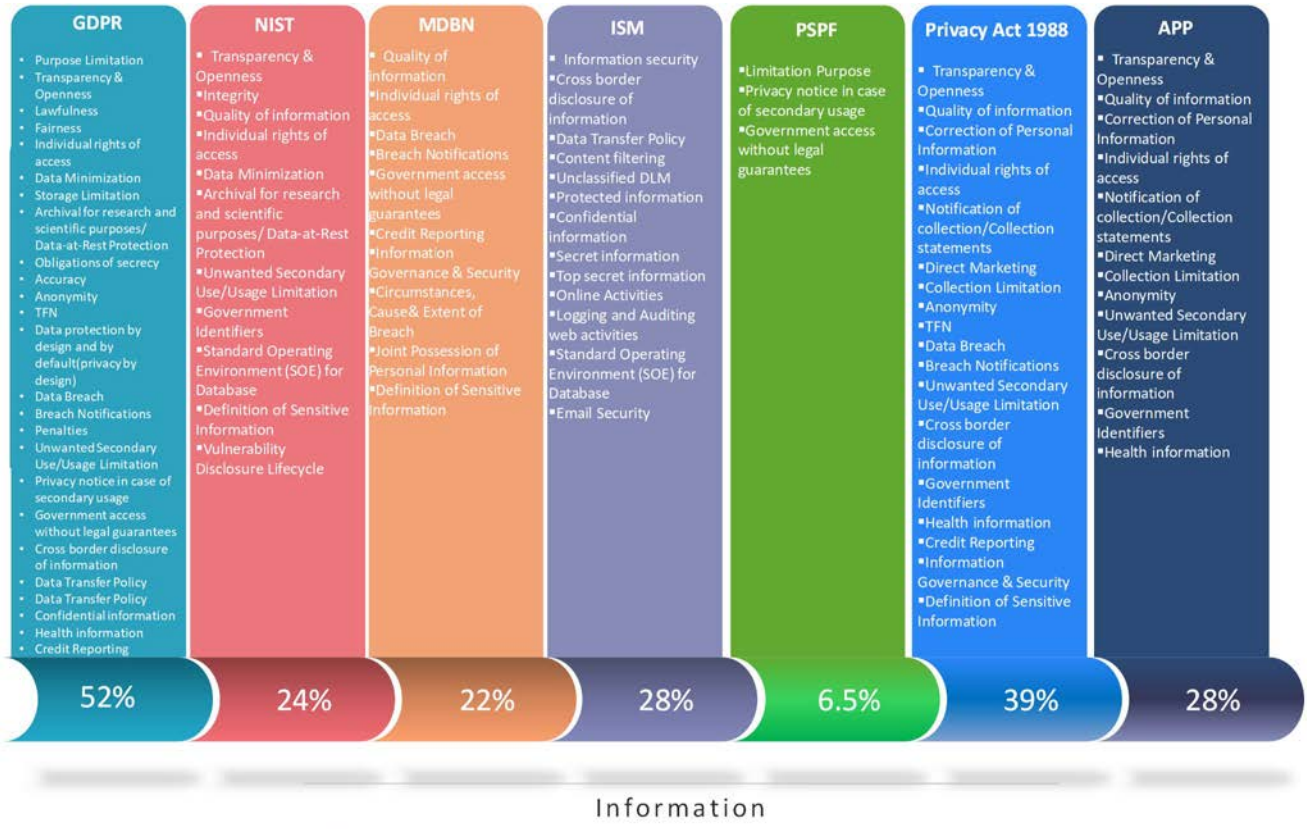

Figure 5: Division of People Layer and Applicability of laws

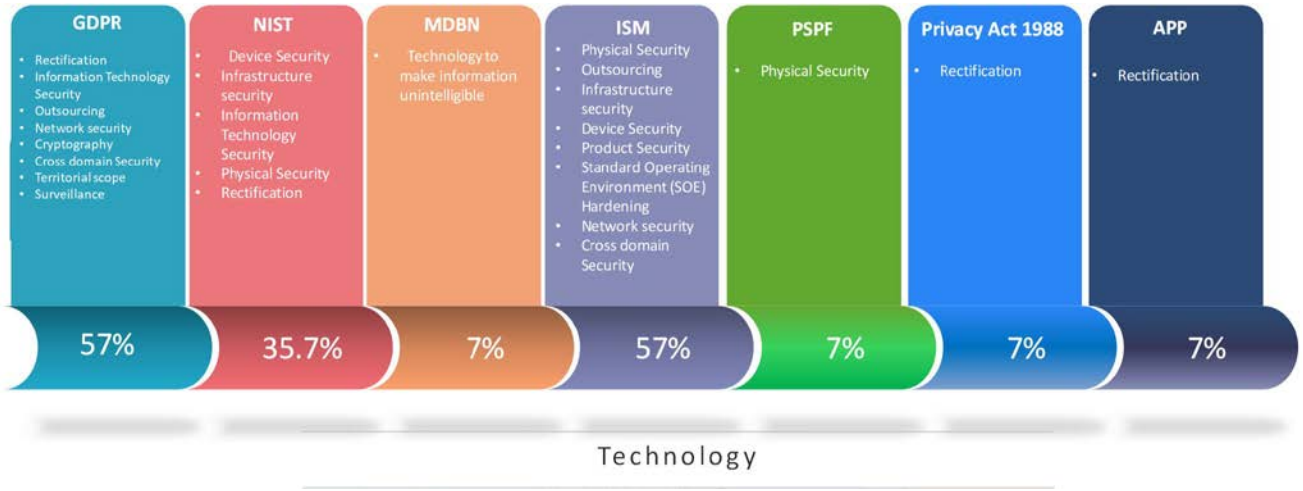

Figure 6: Division of People Layer and Applicability of laws

The score for each layer shows the number of attributes covered by individual law in those layers. For example, APP, PSPF and ISM provide privacy controls for only two attributes in people's layer of digital ecosystem, thus constituting only 8.3% of the total listed attributes. Privacy Act 1988 provides controls for 20.8% attributes, NIST cybersecurity framework gives 25% coverage and MDBN provides solutions against 16.6% attributes. It is evident from the scores that GDPR is the only law that yields maximum coverage (70%). The laws under discussion cover process layer to a lesser extent. APP gives no coverage at all in this layer whereas privacy act has controls for around 11.5% attributes in process layer. PSPF,

ISM and MDBN are applicable to 19.2%, 26.9% and 30.7% of total attributes. In this layer, foreign laws (NIST and GDPR) seem to be more thorough and complete with NIST's applicability to 53.8% elements and GDPR to 34.6% attributes.

Information or data layer is the key layer in digital ecosystem and it provides foundation for many other layers. Hence, the attributes in this layer are multidimensional, some overlapping with the other layers too. For example, when it is being said that information needs to have a purpose limitation, this relates to some process that ensures purpose limitation. In order to attain this attribute information security policy is needed which is one of the attributes of process layer. However, the applicability of the laws under discussion in this study is almost same as it is for other layers. APP (28%), PSPF (6.5%), ISM (28%), NIST (24%) and MDBN (22%) gives coverage to less than 30% of the attributes in information layer. Privacy Act is a bit thorough covering 39% elements, whereas GDPR gives a score of 52% and proves to be the most widespread in this layer. GDPR and ISM possess controls and principles that apply mostly to the technology layer. GDPR has 57% and ISM has 61.5% controls targeting technology related attributes. Rest of the seven laws under review in this paper, i.e. APP, Privacy Act 1988, PSPF, NIST and MDBN each cover 7% of the technology layer attributes.

5 Discussion and analysis

Any business, once established the information to be collected, stored, used or disclosed that may be considered 'personal', 'sensitive' or 'health' information, it then needs to determine which (if any) privacy laws apply to the organisation. This is the most difficult part to figure out which law covers all the aspects of the organization and its business domain. With digital ecosystems, especially there is no law that perfectly covers all the areas throughout the lifecycle. In this study, a review of Australian Privacy laws is conducted according to the criteria mentioned in table 2. The general industry standards and government segments in Australia were analysed against the current information security related guidance, laws, regulations and legislations and a summarized description of the results is presented in figures 1 to figure 6. Researchers can use these figures as a starting point in their understanding of applicable regulation/standard for a specific privacy attribute. It must be taken into account that there are few information security related legal, legislative and regulatory obligations applicable for all layers of DE. Figure 1 highlights the collective coverage of privacy laws under review across the layers.

Australian Privacy Principles (APP) are part of the recent amendment to **Privacy Act 1988(Cth).** This set of APPs upon which Privacy act is based, applies to federal government as well as to private sector organizations. It has ended the complexity and confusion in the application of privacy laws largely (The Privacy Act 1988). 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 (Watts and Casanova, 2018). In this research, we have concluded that APP and privacy act 1988 does not cover many aspects of privacy in digital ecosystem. From the results we can see that APP and privacy act are applicable to 8..3% and 20.3% on people layer, 0% and 11.5% on process layer, 28% and 39% on information layer and 7% each on technology layer. Being a part of any Australian government agency, companies need to be compliant with the mandatory requirements of the **Protective Security Policy Framework (PSPF)** (Sinha 2018). It promotes a risk- managed perspective to privacy. The PSPF is believed to address many challenges impersonated by the recent rise of technology and prominently supplementary threats due to data deluge. Information Security manual is another government standard in Australia that complements PSPF. The manual is the standard that governs the security of government ICT systems. However, with digital ecosystem, there are certain areas where PSPF and ISM lack applicability. According to the results deducted in this study, PSPF and ISM give 8.3% applicability on people layer, which is very low figure. On process, information and technology layers, they offer 19.2% and 27% (process layer), 6.5% and 28% (information layer) and 7% and 57% (technology layers) applicability. **Mandatory data breach notification (MDBN)** 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 (OAIC 2018). This is a very recent law and offers a good coverage on digital ecosystem layers. It has 16.6% control for people layer, 30.7% for process layer, 7% for technology layer and 22% for information layer.

NIST's Cyber Security Framework is a US based framework used by many organisations. It is a prioritised, flexible, repeatable and cost-effective framework to help manage cyber security-related risks (NIST Framework for Improving Critical Infrastructure Cybersecurity 2018). According to our mapping, it is the second most thorough law that has reasonable percentage of controls applicable to each layers of digital ecosystem. It has been found that NIST is applicable to 52% of people layer attributes, 53.8%

of process layers, 24% technology layer and 35.7 percent technology layer. This is a very good percentage as compared to Australian laws. Even better coverage is provided by EU;s GDPR. It has highest coverage on people with 70% attributes covers. Process layer has 34.6% applicability from GDPR, 52% on information layer and 57% on technology layer. 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 **General Data Protection Regulation (GDPR)** (EU GDPR 2018)**.** 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 digital ecosystem 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. No reform activity has considered the impact of Big Data on Australia's privacy laws.

6 Conclusion and future work

This paper presented a comprehensive review and mapping of seven important regulations to clearly understand their support or coverage for designing the contemporary digital ecosystems. The results indicate that the reviewed regulations differ in nature and scope but have some common overlapping areas and gaps, which warrant further research. The results of this study have implications for both researchers and practitioners who have interest in designing and developing secure digital ecosystem, to ensure that important regulatory requirements are identified and are not overlooked. This research has also implications for regulators to make an informed decision about the review or modification of existing regulations to ensure the privacy of information in multi-party digital ecosystems. In a nutshell, this work is intended to help researchers, regulators and practitioners to understand the scope and relevance of each privacy law.

7 References

Attorney-General's Department, A.G.2016. "Protective Security Policy Framework 2016-17 Compliance Report", Attorney- General's Department, Australia, pp.1-11

Australian Cyber Security Centre (ACSC). 2018. Acsc.gov.au, https://acsc.gov.au/ , retrieved: August 5, 2018

Bashir, M.R., and Gill, A. Q. 2016. "Towards an IoT Big Data Analytics Framework: Smart Buildings Systems," *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/Smart City/DSS)*, January, pp. 155-178.

Bowen, Glenn A., 2009, 'Document Analysis as a Qualitative Research Method', Qualitative Research Journal, vol. 9, no. 2, pp. 27-40. DOI 10.3316/QRJ0902027. This is a peer-reviewed article.

Christie, A. & Saadati, R. 2013. "Australia: Big Data, big issues? Is Australian privacy law keepingup?",http://www.mondaq.com/australia/x/254100/data+protection/Big+Data+big+issues+Is+Australian+privacy+law+keeping+up , Retrieved 23 July, 2018.

Commission, A. L. R. 2007. "Review of Australian Privacy Law," *DP* (72), pp. 51-52.

Commission, A. L. R. 2008. "*For Your Information: Australian Privacy Law and Practice*", *Report*. Law Reform Commission.

Commission, A.G.P. 2016." Productivity Commission Data Availability and Use Draft Report", pp.1-652

Croucher, R. 2011. "Australian Privacy Law & Practice - Key Recommendations for Health Information Privacy Reform.", https://www.alrc.gov.au/news-media/2011/australian-privacy-law-practice-key-recommendations-health-information-privacy-refor?print, Retrieved: 13 July, 2018

Cybersecurity, C. I. 2014. "Framework for Improving Critical Infrastructure Cybersecurity," *Framework* (1), p. 11.

Department of Defence, A.G. 2017. “Australian Government Information Security Manual”, Australia, pp. 1-340

Duynstee,C.A.N.L., Haayen,M.J., Kyritsis,D., Ortega-Cordova,L.M. & Samat,S.N.N. 2016. “Synthesis Project Dordrecht Smart City Dordrecht – Identification of Pedestrian Movement Patterns with Wi-Fi Tracking Sensors.” , TUDelft, May 23,2016, pp.1-77

EU. 2018, “General Data Protection Regulation”, https://gdpr-info.eu , Retrieved: 5th June, 2018.

Gill, A. Q. 2015. "Agile Enterprise Architecture Modelling: Evaluating the Applicability and Integration of Six Modelling Standards," Information and Software Technology (67), pp. 196-206.

Gill, A.Q., Smith, S., Beydoun, G. and Sugumaran, V. 2014. Agile enterprise architecture: a case of a cloud technology-enabled government enterprise transformation.

Holt, J., and Malčić, S. 2015. "The Privacy Ecosystem: Regulating Digital Identity in the United States and European Union," *Journal of Information Policy* (5), pp. 155-178.

Joshi, H. 2017. “Security and Privacy in the Digital World”, Deloitte, pp.1-27

Moghe, V. 2003. "Privacy Management–a New Era in the Australian Business Environment," *Information Management & Computer Security* (11:2), pp. 60-66.

NIST. 2018.”Framework for Improving Critical Infrastructure Cybersecurity”, https://doi.org/10.6028/NIST.CSWP.04162018 ,Retrieved: July 2,2018

OAIC, A.G. 1988.”The Privacy Act (1988)”, https://www.oaic.gov.au/privacy-law/privacy-act , retrieved: 12 June, 2018.

OAIC, A.G. 2018. ”Data Breach Preparation and Response”, https://www.oaic.gov.au , Retrieved 1st June 2018.

Patchwork, N.S.W. 2014. “Patchwork is a tool to share practitioner information, not to share client information”, https://www.patchworknsw.net.au/privacy , Retrieved July 23, 2018.

Schmidt, A. 2014. “What is the best definition for “digital ecosystem”?”, Quora

Sinha,G. 2018.”Governance, risk and compliance:2018 trends and predictions.” https://www.itproportal.com/features/governance-risk-and-compliance-2018-trends-and-predictions , Retrieved: July 16, 2018.

Urbiola, P. 2018. “The power of digital ecosystems”, BBVA Research, February, pp 1-3

Watts, D. & Casanova, P. 2018, “Privacy and Data Protection in Australia: a Critical overview (extended abstract)”, https://www.w3.org/2018/vocabws/papers/watts-casanovas.pdf, Retrieved: 5th June, 2018.

YourCause, 2018. “Privacy Policy”, May 2018, pp.1-13

Acknowledgements

This research is funded by the Australian Govt. Research Training Program (RTP). Views expressed herein are however not necessarily representative of the views held by the funders.

Copyright