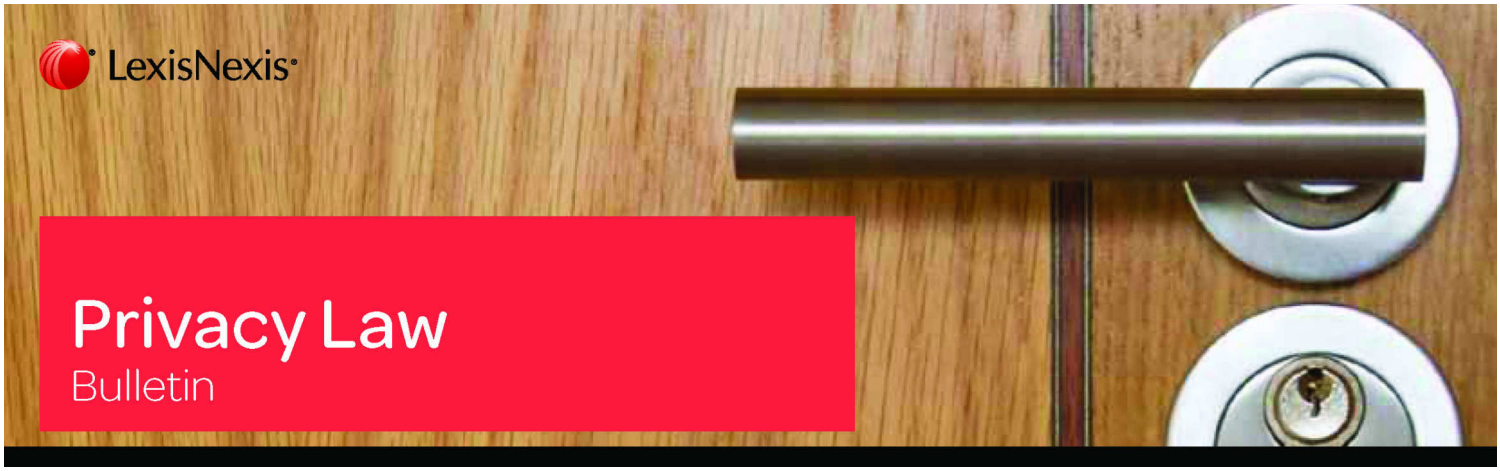

Privacy Law Bulletin

2019 . Vol 15 No 10

Contents

Information contained in this newsletter is current as at March 2019

LexisNexis Butterworths

Privacy Law
Bulletin

Protecting employee data in a post-GDPR world

Dr Ashley Tsacalos *and* ***Monique Azzopardi*** *CLAYTON UTZ*

Introduction

A common source of misunderstanding for Australian employers is the scope and application of the "employee records exemption" under the Privacy Act 1988 (Cth). It is not a blanket exemption from the need to protect employee data and operates in the context of other relevant laws, including the new European Union (EU) General Data Protection Regulation (GDPR).

The intent of this article is to discuss and test the limits and scope of the employee records exemption, especially in light of the new GDPR. It also explores the practical steps that Australian businesses and their human resource departments can take to protect employee data in a post-GDPR world.

Australia's employee records exemption

The employee records exemption is set out in s 7B(3) of the Privacy Act. The effect of it is that organisations governed by the Privacy Act are exempt from compliance with the Australian Privacy Principles (APPs) if their acts or practices are directly related to:

> (a) a current or former employment relationship between the employer and the individual; and
> (b) an employee record held by the organisation and relating to the individual.

An "employee record" is defined as a record of personal information relating to the employment of the employee. It includes health information about the employee and personal information relating to matters such as the engagement, training, disciplining or resignation of the employee, the employee's terms and conditions of employment, the employee's performance, and the employee's banking or superannuation affairs.[1]

Despite the breadth of information that falls within the scope of an employee record, businesses should take caution before relying on the employee records exemption. The exemption is not as far-reaching as it might appear at first blush and does not give employers free rein to do what they wish with an employee's data.

The first important point to note is that the exemption applies to private sector organisations only. Public sector agencies covered by the Privacy Act (such as Commonwealth Government departments and agencies) still need to handle the personal information of their employees in accordance with all applicable APPs.

Secondly, because the exemption only applies to acts and practices of an organisation in relation to its employees, it does not apply to unsuccessful job applicants or to employees and other personnel from external organisations. Importantly, and especially in today's "gig economy", the employee records exemption does not extend to contractors, subcontractors, freelancers and volunteers.

Thirdly, the exemption does not cover all personal information that is created during the course of an employment relationship. Vast amounts of data are generated about employees through the work context. Not all such data will be an employee record; for example, personal emails received from an employee via their work email.

Fourthly, there must be a sufficient nexus with the employment relationship for the employee records exemption to apply. In this regard, employers cannot "do whatever they like with employee records."[2] At the time the employee records exemption was debated in parliament, the then Attorney-General stated:

> The employer must be dealing with the employee records in the context of a current or former employment relationship for the exemption to apply. This means that there is no scope for an employer to sell or otherwise take commercial advantage of the personal information contained in the employee records it holds.[3]

Accordingly, an employer could not rely on the exemption to sell personal information relating to employees for direct marketing purposes.

Lastly, the employee records exemption does not exempt employers from the scope and application of other relevant laws, including those related to workplace relations[4] and surveillance.[5] Common law obligations will also continue to apply, including the employer's duty of care to their employees to prevent psychological injury, which might arise from a data breach involving an employee record.

In the context of worldwide data flows, international laws and regulations are becoming increasingly relevant to the processing and protection of employee data. The GDPR is a case in point.

The GDPR

The GDPR came into force on 25 May 2018. It ushered in significant changes to EU privacy laws and a new standard for privacy compliance. It covers the processing of "personal data", which is information relating to an identified or identifiable natural person.[6] Importantly, the GDPR does not contain an employee records exemption. It also does not include a small business exemption that is equivalent in scope to the one under the Privacy Act.

But my business is based in Australia — why do I need to bother about a foreign law?

It is true that the GDPR will not apply to all Australian businesses. However, its wide extraterritorial application is such that it is impacting many Australian businesses who process personal data of individuals (including employees) in certain contexts. The absence of an office or physical presence within the EU will not, of itself, excuse Australian businesses from the need to comply with the GDPR because of the effect of Art 3(2) of the GDPR, which extends the reach of the GDPR to businesses outside the EU in certain circumstances. Australian businesses should therefore heed the advice of the Office of the Australian Information Commissioner and determine whether the GDPR applies to them and, if applicable, take steps to ensure that their personal data processing practices adhere to the GDPR.[7] The risk of failing to do so is severe. The potential financial penalties for noncompliance with the GDPR are large, including fines of up to €20 million or 4% of an organisation's global annual turnover (whichever is higher) for certain violations. In January 2019, Google LLC witnessed the force of the GDPR when it was confronted with a major financial penalty of €50 million for GDPR breaches.[8]

The regulator is clearly willing to pursue entities outside the EU for contraventions of the GDPR. Indeed, the UK Information Commissioner's Office issued its first enforcement notice under the GDPR against a company located in Canada.[9]

Even where the GDPR does not apply to an Australian business, it may apply to contractors of an Australian business and those who may process personal data (including payroll data) on its behalf. Contractors may therefore try and impose GDPR-specific obligations on Australian entities through contract.

The territorial reach of the GDPR in an employment context

The territorial scope of the GDPR is set out in Art 3 of the GDPR. In broad terms, an Australian business that is a data "controller" or "processor" of personal data (as those terms are defined under the GDPR[10]) is required to comply with the GDPR if it:

a) has an "establishment" in the EU and processes personal data in the context of the activities of the establishment (regardless of whether the processing takes place in the EU)
b) does not have an establishment in the EU, but offers goods or services to individuals in the EU or
c) does not have an establishment in the EU, but monitors the behaviour of individuals in the EU

In an employment context, points a and c above will be most applicable. Unless an employer also offers goods or services to its employees, point b will not usually apply in an employment context. Absent an establishment in the EU, the GDPR would not be triggered simply where the workforce of an Australian business includes EU nationals working in Australia (for example, those on a visa program). This is because EU employees are not physically based in the EU and the processing does not relate to the offer of goods or services to individuals in the EU.

Businesses with an establishment in the EU

Article 3(1) of the GDPR provides that the GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU. The GDPR Articles must be read in light of their associated recitals. Recital 22 indicates that an:

> Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.

Recent guidelines (Guidelines) issued by the European Data Protection Board (EDPB) concerning the territorial scope of the GDPR also provide some clarity about Art 3(1).[11] The Guidelines acknowledge that "the notion of establishment is broad" and note that the presence of one employee or agent may trigger the application of Art 3(1) in certain circumstances.[12] However, there are limits to its reach. For example, "it is not possible to conclude that the non-EU entity has an establishment in the Union merely because the undertaking's website is accessible in the Union."[13]

Each case will be determined on its facts. In an employment context, some examples of activities that may trigger the application of the GDPR by virtue of Art 3(1) are below:

- An Australian food supplier hires salespersons in the EU for the purposes of undertaking its sales and marketing activities in the EU.
- An Australian business has any of its employees on secondment to its subsidiary in the EU.

- An Australian business operates its payroll functions in the EU from an office or branch in the EU.

By virtue of Art 3(1), the GDPR may be triggered in some of the above examples, even if the processing of personal data takes place in Australia or outside the EU.

Based on the Guidelines, it is unlikely that an employer with no establishment in the EU will be caught by the GDPR merely because it utilises a contractor established in the EU to process employee data (for example, to provide a payroll system). However, some GDPR obligations would apply to the contractor in its capacity as a processor of the personal data.[14]

Monitoring the behaviour of an individual in the EU

It is commonplace for businesses to carry out some form of monitoring of their employees, including through the use of:

- technologies that monitor internet and ICT usage
- CCTV or other forms of audiovisual surveillance
- vehicles with tracking devices or GPS
- mobile phones and wearable devices, such as smart watches

For the GDPR to be triggered, the behaviour monitored must:

- relate to a data subject in the EU
- take place within the territory of the EU[15]

Under Art 3(2)(b), it is the location of the data subject that is relevant, not the data subject's citizenship or residence status.

On the face of it, the concept of monitoring seems to be of potentially very broad application. Recital 24 of the GDPR provides some clarification. It states:

> In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

The Guidelines highlight that not every online collection or analysis of personal data of individuals in the EU would be deemed "monitoring". The Guidelines state:

> It will be necessary to consider the controller's purpose for processing the data and, in particular, any subsequent behavioural analysis or profiling techniques involving that data … the tracking of natural persons on the [i]nternet, including the potential subsequent use of profiling techniques, is a key consideration.[16]

The GDPR is clearly focused on particular types of monitoring. That said, the Guidelines also confirm that monitoring is not limited to internet tracking but other types of network or technology that involve the processing of personal data. It could therefore encompass a broad range of activities, including geolocalisation activities, the use of CCTV, online tracking through the use of cookies or other tracking techniques, and the monitoring of an individual's health status.[17]

Case law will confirm the extent to which particular types of monitoring activities may fall within the reach of the GDPR. There is certainly the risk that certain types of employee monitoring may be captured by the GDPR. For example, an Australian business which has no establishment in the EU, but which monitors the behaviour of an individual in the EU (for example, an employee's behavioural patterns while on secondment within the EU) would likely fall within the territorial reach of the GDPR.

The GDPR applies — what does this mean for employee data?

The requirements under the GDPR are similar in many respects to obligations under the Privacy Act. However, there are some core areas of difference. It is beyond the scope of this article to discuss those differences in detail, it will suffice to note some key matters. Under the GDPR, employees have increased rights in relation to their personal data; for example, the right to restrict the processing of their personal data[18] and the right to "data portability" in certain circumstances.[19]

Consent is another area of difference. Under the GDPR, personal data may only be processed if one of the conditions for processing set out in Art 6 applies. Consent is one such basis.[20] Compared with the Privacy Act, the requirements for consent under the GDPR are onerous, including the requirement that it be freely given, specific and informed.[21] It has been stated that it will be difficult to rely on consent in an employment context as employees "are seldom in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship."[22] Entities to which the GDPR applies will therefore need to rely on an alternative method to process employee data; for example, for the employer's legitimate interests under Art 6(1)(f) of the GDPR.

What steps should employers take to protect an employee's data?

The advent of the GDPR is an opportune time for Australian businesses to consider the way that they handle and protect the personal information of their personnel and to reconsider the limits of the employee

records exemption. Even if an Australian business is not affected by the GDPR and can validly rely on the employee records exemption, it should still implement privacy best practices, including compliance with the APPs. Such an approach is recommended by the Australian Fair Work Ombudsman.[23]

Increasingly, the GDPR is seen as the new gold standard for privacy compliance. The failure to protect an employee's data may affect business dealings with EU counterparts and may reflect badly on the organisation's management and protection of personal information more generally. The reputational costs of any loss or misuse of employee data may be significant, especially if it attracts any media coverage.

Employers should take the following steps:

- *Audit*: Employers should audit and assess their processing of employee data throughout their organisation, including the geographical reach of their human resource activities within the EU. This should include an assessment of whether personal data is being processed and any potential links between the activity for which the data is being processed and the activities of any presence of their organisation in the EU.[24] A privacy audit and data mapping exercise will assist businesses to conduct this assessment.
- *Legal basis to process*: Where the GDPR applies, employers should ensure that the processing is for a legal basis under the GDPR. They should also follow the principles of proportionality and data minimisation, including ensuring that the use of personal data is relevant and limited to what is necessary in relation to the purposes for which the data is being processed.[25]
- *Check and update policies and procedures*: Employers should check their existing privacy policies and procedures to ensure they comply with all applicable laws, including, if applicable, the requirements under the GDPR. Employee contracts and consent forms may need to be revisited. Any documentation or procedures that are deficient should be promptly updated.
- *Training*: Employers should ensure that their personnel who handle, or have access to, the personal information of employees (including human resource personnel) are familiar with their legal obligations in relation to employee data under all relevant laws. The training should cover the scope and application of the employee records exemption and the effect of laws such as the GDPR.
- *Ongoing review*: Employers should ensure that, as an ongoing business as usual practice, they regularly audit the ways that they process employees' personal information. At the same time, employers should review and test the effectiveness of their systems and processes in relation to the security and protection of personal information, including employee data. Where the GDPR applies, a data breach involving employee data may be notifiable.

Dr Ashley Tsacalos
Partner
Clayton Utz
atsacalos@claytonutz.com
www.claytonutz.com

Monique Azzopardi
Senior Associate
Clayton Utz
mazzopardi@claytonutz.com
www.claytonutz.com

Footnotes

1. See s 6(1) of the Privacy Act for a full definition of "employee record" and further examples of employee records.
2. Commonwealth, *Parliamentary Debates*, House of Representatives, 8 November 2000, 22370 (D Williams, Attorney-General) https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22chamber/hansardr/2000-11-08/0008%22.
3. Above n 2.
4. For example, the Fair Work Act 2009 (Cth) and the Fair Work Regulations 2009 (Cth) regulate the retention of employee records and the form and content of such records. This legislation also provides employees with some rights in relation to their employee records, including the right to inspect and copy records that relate to them.
5. At present, Australia does not have uniform laws regulating employee surveillance and different laws will apply in different states and territories. One such relevant law in New South Wales is the Workplace Surveillance Act 2005 (NSW). It regulates employee surveillance within the workplace, including computer surveillance.
6. GDPR, Art 4(1).
7. Office of the Australian Information Commissioner, Privacy business resource 21: Australian businesses and the EU General Data Protection Regulation, updated June 2018, www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-21-australian-businesses-and-the-eu-general-data-protection-regulation.
8. CNIL "The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC" (21 January 2019) www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.

9. Information Commissioner's Office, Enforcement Notice: The Data Protection Act 2018 Part 6, Section 149, 24 October 2018, https://ico.org.uk/media/action-weve-taken/enforcement-notices/2260123/aggregate-iq-en-20181024.pdf.
10. Above n 6, Art 4.
11. EDPB "Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) — Version for public consultation" (adopted on 16 November 2018) https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf. It is anticipated that a finalised version of the Guidelines will be issued later this year. The Guidelines may change, which may alter certain content in this article.
12. Above n 11, at 5.
13. Above n 11, at 5.
14. Above n 11, at 10–11.
15. Above n 6, Art 3(2)(b).
16. Above n 11, at 18.
17. Above n 11, at 18.
18. Above n 6, Art 18.
19. Above n 6, Art 20(1).
20. Above n 6, Art 6(1)(a).
21. Above n 6, Art 4(11).
22. Article 29 Data Protection Working Party "Opinion 2/2017 on data processing at work" (adopted on 8 June 2017) 4 https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169.
23. Fair Work Ombudsman "Best Practice Guide: Workplace Privacy" (May 2014) 2 www.fairwork.gov.au/how-we-will-help/templates-and-guides/best-practice-guides/workplace-privacy.
24. Above n 11, at 7.
25. Above n 22, at 23–4.

Is your financial data safe? Comprehensive credit reporting and its impact on financial privacy

Andrea Beatty *and* ***Chelsea Payne*** *PIPER ALDERMAN*

Comprehensive credit reporting (CCR) is a positive credit reporting system to improve the quality of credit decisions by increasing the level of available information. The government's original intention was to commence CCR on 1 July 2018. However, at the time of writing, the National Consumer Credit Protection Amendment (Mandatory Comprehensive Credit Reporting) Bill 2018 (Cth) (exposure draft) has been passed by the House of Representatives and is currently before the Senate. During the legislation's consultation process, numerous submissions raised concerns about the impact increased credit reporting will have on the financial privacy of consumers. This article will provide a brief overview of CCR, and then explore the benefits of CCR and the impact CCR will have upon individuals' financial privacy. However, even though the exposure draft has yet to pass parliament, the major credit providers have started providing CCR data to credit reporting bodies.

CCR in a nutshell

CCR represents a shift from purely negative credit reporting to recording both positive and negative credit information on credit histories. Under the exposure draft, eligible licensees (being large authorised deposit-taking institutions (ADIs) and their subsidiaries) are required to disclose mandatory credit information to eligible credit reporting bodies (such as illion, Equifax and Experian) on eligible accounts.[1]

Additional information which will be available on consumers' credit reports under CCR includes 24 months of repayment history, dates accounts are opened and closed, types of credit accessed, credit limits and how often consumers pay bills on time.[2] When CCR commences, eligible licensees will be required to supply information for at least 50% of their eligible accounts by the first 1 July that they are an eligible licensee, with the bulk supply of remaining information to be provided within 90 days of that 1 July.[3]

CCR was not originally intended to be a mandatory regime. In 2017, the government announced that it would mandate CCR if credit providers failed to meet a threshold of 40% data reporting by the end of the year. In November, the then Treasurer Scott Morrison announced that the uptake of CCR had been less than 1%,[4] leading to the introduction of the mandatory CCR regime.

Benefits of CCR

There are a number of benefits to CCR through creating a more balanced and transparent credit reporting system. CCR will ultimately benefit consumers with positive credit histories by highlighting good behaviour. Those consumers which have experienced adversity will also experience faster recovery of their credit scores through positive reporting.

CCR will result in improved risk assessment and responsible lending for credit products,[5] as credit providers will have access to more accurate data. This will also reduce the levels of excessive debt and default rates, as credit providers will be in a better position to determine whether a consumer should be assuming additional debt.[6]

Finally, CCR is likely to promote competition and efficiency in the market,[7] as smaller credit providers will have access to comprehensive information that is typically held by the larger banks.

Privacy implications

Throughout the development of CCR in Australia, questions have been raised about the effects on an individual's right to privacy. CCR differs to the open banking concept in this way, as consumers have no input as to whether their data is shared. Although increased data sharing will be advantageous for consumers such as those with limited credit histories, it could not be advantageous for others.

The underlying concept of CCR will mean that more data is available to credit reporting bodies. This will be beneficial to consumers such as young people, as it will enable them to develop a more comprehensive credit history in a short period of time. This can be of particular assistance for those wishing to access low-interest credit with limited, albeit positive, credit histories. However, critics argue that the increased data

accessibility will result in inaccuracy and errors in data made available due to the high volumes of data required to be input into the system.[8] In the alternative, proponents of CCR believe that this will lead to greater data accuracy, as eligible licensees will have greater familiarity of the process.[9]

Data security has also been raised as a major concern for CCR, as credit reporting bodies will have unrestricted access to consumers' data in the database. The NSW Consumer Credit Legal Centre believes that this type of access could lead to issues including identity fraud and potential misuse of data for marketing purposes.[10]

Privacy concerns also arise in regard to hardship flags, and whether these will be viewable by credit reporting bodies. This may create issues where a customer becomes reluctant to contact their credit provider to request hardship assistance out of concern that this information will become available through CCR.[11] Even if hardship flags are not viewable through CCR, it is likely that credit reporting bodies will still be able to identify when these instances occur through the data available to them.

Summary

CCR will represent a significant change to Australian credit reporting. CCR will have its benefits for consumers, including highlighting positive credit behaviour and more responsible lending from credit providers. However, the sharing of additional information will mean that individuals will lose their right to financial privacy. Obvious implications of this are potential data inaccuracies and having hardship information potentially available to credit reporting agencies.

The introduction of open banking and CCR coupled with the final report of the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry due this year will present significant changes to the finance industry, so this will be an interesting space to watch.

Andrea Beatty
Partner
Piper Alderman
abeatty@piperalderman.com.au
www.piperalderman.com.au
www.andreabeatty.com.au

Chelsea Payne
Law Graduate
Piper Alderman
cpayne@piperalderman.com.au
www.piperalderman.com.au

Footnotes

1. National Consumer Credit Protection Amendment (Mandatory Comprehensive Credit Reporting) Bill 2018 (Cth), s 133CR.
2. GetCreditScore, Everything To Know About Comprehensive Credit Reporting, 21 June 2018, www.getcreditscore.com.au/articles/everything-to-know-about-comprehensive-credit-reporting/.
3. Above n 1, s 133CR.
4. S Morrison "Mandating comprehensive credit reporting" media release (2 November 2017) http://sjm.ministers.treasury.gov.au/media-release/110-2017.
5. Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* (2008) Vol 3, Pt G, Ch 55 www.alrc.gov.au/publications/For%20Your%20Information%3A%20Australian%20Privacy%20Law%20and%20Practice%20%28ALRC%20Report%20108%29%20/55-more-co.
6. Above n 5.
7. Above n 5.
8. Galexia Pty Ltd, Submission PR 465 to Australian Law Reform Commission, *Inquiry into Privacy Law and Practice*, 13 December 2007; Office of the Privacy Commissioner, Submission PR 281 to Australian Law Reform Commission, *Inquiry into Privacy Law and Practice*, 13 April 2007.
9. ANZ, Submission PR 291 to Australian Law Reform Commission, *Inquiry into Privacy Law and Practice*, 10 May 2007; Veda Advantage, Submission PR 272 to Australian Law Reform Commission, *Inquiry into Privacy Law and Practice*, 29 March 2007; MasterCard Worldwide, Submission PR 237 to Australian Law Reform Commission, *Inquiry into Privacy Law and Practice*, 13 March 2007; GE Money Australia, Submission PR 233 to Australian Law Reform Commission, *Inquiry into Privacy Law and Practice*, 12 March 2007.
10. Consumer Credit Legal Centre (NSW) Inc, Submission PR 28 to Australian Law Reform Commission, *Inquiry into Privacy Law and Practice*, 6 June 2006.
11. ANZ, Submission to Attorney-General's Department, *Consumer Credit Reporting and Hardship Review*, June 2018 3 [8] www.ag.gov.au/Consultations/Documents/financial-hardship/submission-anz.pdf.

Blockchain and the Australian Privacy Principles: never the twain shall meet

Michael Rivette *CHANCERY CHAMBERS and* ***Adam Lodders*** *NETWORKED SOCIETY INSTITUTE, UNIVERSITY OF MELBOURNE*

In this article we explore the emergence of blockchain, its development and use before turning to the challenge the Australian privacy regime places on effective implementation and uptake. We will examine the limits imposed upon blockchain by Australia's privacy law for use and storage of personal information. We will also explore the main areas of conflict between privacy and blockchain: correction, data breaches and jurisdiction.

As the law currently stands, entities that are covered by the Australian Privacy Principles (APPs) should be extremely cautious when storing personal information on blockchains, as it may result in an arrangement that makes compliance with the APPs impossible.

Introduction

On 31 October 2008, a pseudonymous programmer (or programmers) going by the name Satoshi Nakamoto published "Bitcoin — A Peer to Peer Electronic Cash System",[1] which became known as the "White Paper". In the years following its publication, Satoshi Nakamoto shared with the world not only his vision but the code to build it.

And so, the world was introduced to cryptocurrencies, through a platform that allowed for information, transactions and assets to be passed and recorded in a way that avoided banking institutions and government regulation. Underpinning the platform was a system known as blockchain, which allowed for networks to timestamp transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record *that cannot be changed* without redoing the proof-of-work and altering all subsequent blocks; a near impossible task.

As revolutionary as cryptocurrencies have been, it is the underlying blockchain technology, that is set to change the way many transactions occur, are recorded, and verified.

Data written on a blockchain is virtually impossible to change, and as blockchains may contain personal, confidential and/or sensitive information about an individual, blockchain technology and privacy are in inherent conflict. The architecture, design and use of blockchain technologies have therefore followed the path of many technological innovations, which simply outpace the legal protections.

This is true in Australia, where the current legal protection for privacy is primarily the Privacy Act 1988 (Cth) (Privacy Act), which imposes a range of requirements relating to the regulation of privacy and handling of personal information by organisations, via the APPs.[2] However, the Privacy Act and the APPs, assume a centrally controlled depository of personal and/or sensitive information, and are therefore inherently inadequate in a blockchain world.

Blockchain: context, operation and use

Blockchain has come a long way from its peak in 2017, where cryptocurrencies were all the rage.[3] Prices for cryptocurrency peaked in December 2017, with 1 Bitcoin worth $26,802.[4] Since then prices have fallen quite dramatically with 1 Bitcoin losing more than half its value. Currently, Bitcoin is valued at $5,041.[5] This price has been constant, hovering around the $5,000 — $10,000 mark since May 2017. The hype accompanying blockchain and cryptocurrencies stated that it would revolutionise the economy. While cryptocurrencies have not displaced existing fiat money by any perceptible order — we still need to use Australian dollars to purchase a coffee — there has been great interest in the potential of the underlying technology — blockchain.

In 2008, the Bitcoin White Paper proposed a currency free from centralised state control.[6] This was in the wake of the Global Financial Crisis and the objective of Bitcoin was to create a medium of exchange that was free from interference and control by any government. Bitcoin was designed as a decentralised system to overcome the problem facing digital transactions, how to trust individuals in a trustless environment. The most innovative aspect of Bitcoin was the mechanism to manage and record transactions — the blockchain.

Blockchains are distributed ledgers that store data across a number of different hosts. In the Bitcoin context, they allow the recording and processing of

transactions across a network preventing double spending when all the participants do not need to trust one another.[7] The data is written to blocks, which are chained together using advanced mathematics, with a copy distributed across all number of computer hosts, or nodes, on the network. The writing of data and linking into chains creates a distributed network of databases, all with the same data. Each node of the blockchain is kept in sync via a number of protocols, which vary depending upon the flavour of the installation. Access to this network can either be public, open to anyone with the requisite compute power to host a node, or permissioned with copies of the blockchain only available to a select few individuals.

There are currently a number of use cases for blockchains across a number of industry verticals including payments, supply chains trade, healthcare and insurance.[8] There has been much potential about using blockchain across financial services.[9] However, none have yet seen widespread adoption. The key feature of blockchains is their ability to operate in a distributed manner. This approach sees a copy of all data is recorded to each node across the network creating multi-records, stored in a number of places, where no single node has the ability to correct or erase the data and information.

Blockchain and Australian Privacy Law

The Privacy Act places limits on the protection of personal information in Australia. As we have stated earlier, the architecture of blockchain is in inherent conflict with the APPs. Specifically, there are two main areas of concern, the first regarding the management of personal information, the second relates to access and control by the record keeper.

Management of personal information

The APPs provide the capacity for individuals to request correction of personal information held about them.[10] The data structure of blockchains is immutable. The problem that blockchain solves, trust in a trustless environment, is achieved through all parties having a copy of the record and being able to verify transactions. Correcting personal information recorded on the blockchain means rewriting the whole blockchain. This cannot occur unless over 50% of the network nodes agree. To achieve this requires a level of trust between blockchain participants. Introducing trust, through a collective, or a third party, fundamentally alters the requirements for using a blockchain, and is inconsistent with its vision, platform, basic principles and objectives.

This also arises in the case of deletion. Should personal information no longer be held by an APP entity for a specific purpose, then the APPs impose an obligation that are reasonable in the circumstances to destroy the information.[11] Similarly, in the European Union the General Data Protection Regulation allows individuals to erase information held about them on request.[12] As we noted above, correction of records runs counter to the nature of the blockchain, which is a record of all transactions. In practice, this makes it virtually impossible to delete.

The APPs relating to correction and deletion have an additional requirement of "reasonableness" imposed upon the data controller. Does the fact that through using blockchain the minimum required would be to seek to gain consensus across the network to rewrite the blockchain before disgorging, collecting or using information? Or given that there is specific choice made by an organisation to use blockchain as opposed to other alternative data structures, then does reasonableness relates to capacity to control as a result of a choice? The answer to these and many more questions raised by this technology, are currently unclear, which further reinforces the incompatibility of Australian privacy laws with blockchain.

Access and control

The second main area where blockchain is in conflict with the APPs relates to access and control. The open blockchain networks are distributed. Each node that joins the network contains a copy of the whole blockchain, this includes any data written on the blockchain. These can be located anywhere that has access to an internet connection. Currently there are protections relating to the transfer of data across jurisdictions.[13] The requirement places a condition that offshoring data needs to be done in accordance with the APPs. However, this can be circumvented by seeking consent.[14] Therefore, the use of blockchain by an organisation is likely to require a new and updated consent regime, with the individual who provides their personal information. This could only occur if the organisation has that direct contact with the individual at the time of collection and is not merely a collector of information through a chain that is already established.

Breach

A final consideration relates to data breaches. Specifically, the new notifiable data breach scheme that came into effect in February 2018. The data breach regime establishes a requirement for entities to disclose when there is unauthorised access, or disclosure of information,[15] that would result in serious harm to individuals.[16] The data breach scheme places obligations to prevent individuals from suffering serious harm. The term "serious harm" is not defined, but from general law, and cases relating to privacy matters, we know that

compensable harm can include psychological, emotional, physical, reputational, or economic harm or loss. Assessment is based upon a reasonable person who applies contemporary standards of morals and behaviour and is of ordinary sensibilities.[17] In relation to blockchain, the distributed nature of the network means that the record keeper does not have control as to the operation of other nodes. Additionally, given that upon the establishment of a node the whole record is disclosed to an unknown third party, it is a likely disclosure of personal information, therefore, each potential transfer of data outside the control of the record keeper on the blockchain has the capacity to become a data breach, depending upon the degree of harm caused from the breach.

Conclusion

As it currently stands, blockchain is incompatible with the APPs. The problem that blockchain seeks to solve, enabling trust in a trustless environment, runs counter to the requirement of record-keepers ensuring the security, protection and control of data in their care. The nature of the data structure means that correction and rewriting of data is not practically available.

Further, a distributed network of multiple nodes means that organisations lose control and might be liable for any data breaches that arise relating to information inadvertently disclosed to and by any of the nodes. Use of a trustless environment to store personal information provided to an organisation therefore runs counter to the principles of privacy protection, including "responsible and transparent handling of personal information".[18] Use of blockchain outside the control of an organisation raises serious issues of compliance under the Privacy Act and necessarily involves considerations by organisations of potential risk or liability under the tort of negligence, in equity for breach of confidence, or the consumer protection laws and legislation.

Michael Rivette
Barrister
Chancery Chambers
rivette@chancery.com.au
www.chancery.com.au

About the author

Michael Rivette is a barrister at the Victorian Bar. He is listed in ***Best Lawyers*** *in 2019 in the field of Privacy and Data Protection, is the co-author of the Australian sections of the UK text Tugendhat and Christie* ***The Law of Privacy and the Media****, and a co-author of* ***Remedies for Breach of Privacy****.*

Adam Lodders
Executive Officer
Networked Society Institute, University of Melbourne
adam@adamlodders.net

Footnotes

1. Bitcoin, Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, available at https://bitcoin.org/en/bitcoin-paper.
2. The Australian Privacy Principles apply to APP entities which are defined in s 6(1) of the Privacy Act 1988 (Cth).

   Organisation is defined broadly including individuals, body corporate or partnership or any other unincorporated association or a trust. There is an exemption for small business operators with an annual turnover of less than $3 million, except if they are health service providers or commonwealth contractors.
3. B Barrett, "Blockchain: Lucrative Buzzword or Legitimate Game Changer?" *Pursuit*, 17 May 2018 https://pursuit.unimelb.edu.au/articles/blockchain-lucrative-buzzword-or-legitimate-game-changer.
4. BTC Markets Pty Ltd, www.btcmarkets.net date 16 December 2017.
5. BTC Markets Pty Ltd, www.btcmarkets.net date 18 February 2019
6. Above n 1.
7. E Mik, "Smart contracts: terminology, technical limitations and real world complexity" (2017) 9 *Law Innovation and Technology* 269, 275.
8. IBM, "Let's go beyond blockchain use cases to real blockchain networks" www.ibm.com/blockchain/use-cases/ accessed 12 October 2018.
9. Deloitte, "5 blockchain technology use cases in financial services" www2.deloitte.com/nl/nl/pages/financial-services/articles/5-blockchain-use-cases-in-financial-services.html.
10. Privacy Act, Australian Privacy Principle (APP) 13.1(ii).
11. APP 11.2.
12. General Data Protection Regulation — Article 17. For a detailed discussion about blockchain and the GDPR see: M Finck "Blockchains and Data Protection in the European Union" (2018) *Max Planck Institute for Innovation and Competition Research Paper* No. 18-01.
13. APP 8.
14. APP 8.2.
15. Privacy Act, s 26WE(2)(a)(i).
16. Privacy Act, s 26WE(2)(a)(ii).
17. *ABC v Lenah Game Meats* (2001) 208 CLR 19; 184 ALR 113; [2001] HCA 56; BC200106150 at [42].
18. Privacy Act, s 2A(d).

Privacy Law
Bulletin

Different regions, similar focus: APAC and EMEA narrow in on data subject rights in different regulatory approaches

David Marcus *STATE STREET*

Data privacy is one of the hottest regulatory topics in Asia-Pacific (APAC). One of the issues, however, is that APAC has a number of different approaches to data security compared to the European Union (EU) and North America (NA), and it is important to ensure we do not fall into any pitfalls when advising our business units. This article briefly outlines:

- the common thread with Australian and APAC privacy regulation: greater attention on the rights of data subjects
- the main differences between the Europe, the Middle East and Africa (EMEA) and APAC approaches
- key recommendations for practitioners

The common thread with Australian and APAC regulation: attention on the rights of data subjects

Rights of data subjects are not a new development. Many international instruments have attempted to harmonise privacy laws with respect to the rights of data subjects perhaps most notably during the 2009 "Madrid Resolution" on international privacy standards.[1] Globally, regulatory interest on data subjects is high due to increasing powers and requirements in the EU or the European Economic Area (EEA), and rapidly evolving privacy law responses in APAC. In 2018, scandals in relation to Facebook, Cambridge Analytica and others have created heightened sensitivity by regulators about whether, and in what circumstances, data may be shared with third parties and what protections could be put in place. For example, the Facebook scandal has led to new privacy laws in the state of California which will come into force on January 2020.

Across APAC, the past few decades have experienced promulgation of the Organisation for Economic Co-operation and Development (OECD) model privacy laws[2] that are constantly evolving alongside the rapidly evolving technology market. Against this backdrop is a market convergence of user interfaces on the one hand and functional financial compliance on the other. Whilst the OECD "Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data" (OECD Privacy Guidelines) have been key to shaping global laws on privacy, the two main regional frameworks on data protection in APAC are the "ASEAN Framework on Personal Data Protection"[3] and the "APEC Privacy Framework".[4] Both have been implemented ad hoc across APAC. The Groupe Speciale Mobile Association (GSMA), which represents the interests of mobile operators worldwide, has called for a Pan-Asian response to data privacy across APAC with less regulatory restrictions. It is yet to be seen whether APAC regulators will formalise a regional privacy framework on data privacy in the same way we have seen with the EU's General Data Protection Regulation (GDPR).[5]

Australia's privacy laws are perhaps an exception to these developments and are one of the most pronounced examples of early adoption and industry harmonisation. In Australia, both public and private sector organisations that have an annual turnover of over $3 million have obligations under the Privacy Act 1988 (Cth), including under the Australian Privacy Principles (APPs) which regulate the collection, use and storage of personal information about individuals with whom entities deal. Clause 24 of the 2013 Code of Banking Practice specifically cites duties that banks owe to data subjects under the Privacy Act. APP entities are defined as all businesses subject to the Privacy Act. Such entities must have a privacy policy which specifies, among other things:

- the kinds of personal information that the business collects and holds
- how the business collects and holds personal information
- the purposes for which the business collects, holds, uses and discloses personal information
- how an individual may access and seek correction of personal information that is held about them

On 13 February 2017, the Commonwealth Government passed the Privacy Amendment (Notifiable Data

Breaches) Act 2017 (Cth) which became effective on 22 February 2018. Unlike the GDPR, privacy obligations under the Privacy Act and the APPs are only triggered for businesses that have a turnover of greater than $3 million per annum (no such exemption applies to the GDPR). Currently, parliament is also considering a new "Consumer Data Right" Bill which would provide consumers with greater rights to access data and allow third parties to do so. The Treasury Laws Amendment (Consumer Data Right) Bill 2018 (Cth) is under consideration and has not been enacted yet.

The main differences between the EMEA and APAC approaches to data security

Most companies have in place an Intergroup Agreement that addresses EU requirements on the GDPR. The GDPR formalises a strict framework for data protection under its jurisdiction and sets out circumstances in which a privacy impact assessment (PIA) must be carried out. Under the GDPR, one key proposition is that one Data Protection Authority (DPA) from any EU jurisdiction may act as the counterpart on behalf of all others in the EU.

Despite the same focus on data subjects in EMEA and APAC, we cannot "paint with the same brush" as the GDPR when it comes to Australia or the rest of APAC in relation to privacy regulations. Some regulators across APAC have increased their powers and have the ability to issue stringent restrictions on processing personal data where there has been a violation. Regulators in APAC, particularly in Australia, Singapore and Hong Kong, have focused more on enforcement through fines and "naming and shaming" rather than through restriction orders. In APAC, PIAs are required under patchwork privacy regulations in some jurisdictions. APAC does not have a comparable "no wrong door" regime (as per the GDPR).

A snapshot of a few key regional differences in APAC's implementation of privacy regulations:

- *Hong Kong*. Hong Kong has a reasonable data privacy framework in the form of the Personal Data (Privacy) Ordinance cap 486. The Privacy Commissioner recently reissued guidance on Privacy Management Programmes (PMPs). In terms of PIA, the key requirement of the guide is for all companies to maintain and update a PMP. The "Privacy Management Programme: A Best Practice Guide"[6] is recommendatory guidance and a revision of the 2014 guide.[7] In 2010, the Privacy Commissioner also took the unprecedented step of making recommendations which aimed to restrict data collection practices of the Octopus group of companies with application to all data controllers. The Octopus reward card program unlawfully collected and sold personal data to other businesses for marketing purposes. The report[8] made a number of key recommendations including that the company should not collect certain types of data such as sensitive information (Hong Kong identity card, and month and year of birth), and that appropriate mechanisms should be put in place on the company due to lack of observance of cross-border data transfer risks. As recent as October 2018, the Cathay Pacific data leak affecting 9.4 million customers has once again highlighted the need for greater regulation and greater scrutiny of privacy programs and breach notifications.
- *Singapore*. Singapore has one of the strongest data privacy frameworks in APAC in the form of the Personal Data Protection Act 2012 (PDPA). The PDPA framework is built around the concepts of consent, purpose and reasonableness. Organisations may collect, use or disclose personal data only with the individual's knowledge and consent (subject to certain exceptions) for a purpose that would be considered appropriate to a reasonable person in the circumstances. The Cybersecurity Act 2018, which was passed by the Singapore Parliament on 5 February 2018, came into force on 31 August 2018. The new law creates a regulatory framework for the monitoring and reporting of cybersecurity threats to essential services in Singapore through the appointment of the Commissioner of Cybersecurity. It also creates a licensing regime that will require certain data security service providers in Singapore to be registered.
- *Malaysia*. Cross-border data transfers are currently a hot topic. The Department of Personal Data Protection issued a draft "White List" of cross-border transfer havens, which will shortly be approved. The department issued the draft of the Personal Data Protection (Transfer Of Personal Data To Places Outside Malaysia) Order 2017 which forms part of the consultation paper.[9] Until this is released, specific consent is required from all data subjects along with maintaining records of such consent from each subject. After the White List is issued, data controllers will be able to perform cross-border data transfers out of Malaysia to any other country on the approved list without such consent requirements.
- *China*. The implementation of the new China Cybersecurity Law by the end of December 2018 may place additional obligations on countries with cross-border business with China. The Cyberspace

Administration of China (CAC) is likely to issue guidance which will provide greater protection of data while at the same time maintaining a regime for commercial use with consent.

- *South Korea*. South Korea continues to have one of the most innovative and strictest data privacy regimes in Asia. The right to privacy is enshrined in South Korea's Constitution (unlike other regimes in APAC). 2016 saw a comprehensive tranche of data privacy amendments aimed at strengthening informed consent of data subjects through the Act on Promotion of Information and Communications Network Utilization and Information Protection (Network Act) and the Personal Information Protection Act (PIPA).

Some useful tips for avoiding pitfalls of painting with the same brush

Five key tips for practitioners in legal and compliance are as follows:

Key message on APAC privacy	**Key recommendation**
APAC has a number of divergent and non-comparable legal systems with polarisation from very little to very highly regulated data privacy regimes which are changing rapidly. While GDPR provides a robust extraterritorial framework, it is only applicable in certain circumstances. The approach of APAC regulators is to try to reach a convergence but there is not a meeting of the minds on several areas including enforcement, application and penalties.	The key message to remember regarding APAC privacy is that we cannot fall into the trap of painting with the same brush on privacy.
Data privacy laws are changing rapidly in APAC as the region "comes of age" on privacy and realises the importance of data security to all commercial transactions.	Keep abreast of developments by reading updates from local privacy commissioners and industry papers which may also provide advice on how your organisation may engage with proposed new privacy regimes in the near future.
Notification requirements and standards for notification on breach of data privacy laws are different in each jurisdiction in APAC and are not harmonised in the same fashion as under the GDPR which requires strict standards and a 72-hour notification window.	It is imperative to have a privacy program which accommodates a breach management framework with appropriate mitigation and advisory support based on the guidelines issued by each privacy regulator where there is a nexus with a certain jurisdiction.
Privacy by design is perhaps one of the few examples where EMEA, NA and APAC have experienced a convergence. The concept of privacy by design focuses on the need for privacy consideration to be built into processes and systems where personal data is processed — from the outset. A PIA is an integral part of privacy by design and is carried out to identify and minimise privacy risks since it is considered best practice by privacy regulators globally.	New projects must be appropriately vetted to ensure their components go through a PIA with roles between privacy officers, legal and compliance, appropriately set out in a policy or framework.
In APAC, there are a number of obligations in play by different regulators which have created patchwork requirements around the transfer of personal data.	There is a "positive list" of countries' approach to data transfers in some APAC jurisdictions, whilst others focus on obtaining the consent of data subjects for handling third-party data transfers. Keep on top of such developments via subscription to all regulator circulars.

The views expressed in this article are those of the author alone and do not represent the views of any organisation.

David Marcus
Vice President
State Street
www.statestreet.com

About the author
David Marcus is currently working in a regional Asia-Pacific role at State Street. He has worked as a lawyer and consultant for public and private sectors, including at the United Nations, with experience in trade and investment, privacy, banking and sustainable development.

This article originally appeared in Australian Banking & Finance Law Bulletin Vol 34 No 9.

Footnotes

1. 31st International Conference of Data Protection and Privacy Commissioners "Data protection authorities from over 50 countries approve the 'Madrid Resolution' on international privacy standards" (6 November 2009) www.privacyconference2009.org/media/notas_prensa/common/pdfs/061109_estandares_internacionales_en.pdf.

2. OECD "The OECD Privacy Framework" (2013) www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.
3. Association of Southeast Asian Nations "ASEAN Framework on Personal Data Protection" (2016) https://asean.org/wp-content/uploads/2012/05/10-ASEAN-Framework-on-PDP.pdf.
4. Asia-Pacific Economic Cooperation "APEC Privacy Framework" (2015) www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015).
5. The GDPR (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the EU.
6. Office of the Privacy Commissioner for Personal Data (Hong Kong) "Privacy Management Programme: A Best Practice Guide" (August 2018) www.pcpd.org.hk/pmp/files/pmp_guide2018.pdf.
7. Office of the Privacy Commissioner for Personal Data (Hong Kong) "Privacy Management Programme: A Best Practice Guide" (February 2014) www.pcpd.org.hk/pmp/files/PMP_guide_e.pdf.
8. Office of the Privacy Commissioner for Personal Data (Hong Kong) *The Collection and Use of Personal Data of Members under the Octopus Rewards Programme run by Octopus Rewards Limited* (2010) www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/R10_9866_e.pdf.
9. Department of Personal Data Protection "Personal Data Protection (Transfer Of Personal Data To Places Outside Malaysia) Order 2017" Public Consultation Paper No 1/2017 www.pdp.gov.my/images/pdf_folder/PUBLIC_CONSULTATION_PAPER_1-2017_.pdf.

For editorial enquiries and unsolicited article proposals please contact Vida Long at vida.long@LexisNexis.com.au or (02) 9422 2323
Cite this issue as (2019) 15(10) *PRIVLB*
SUBSCRIPTION INCLUDES: 10 issues per volume plus binder www.lexisnexis.com.au
SYDNEY OFFICE: Locked Bag 2222, Chatswood Delivery Centre NSW 2067
CUSTOMER RELATIONS: 1800 772 772
GENERAL ENQUIRIES: (02) 9422 2222
ISSN 1449-8227 Print Post Approved PP 243459/00067 This newsletter is intended to keep readers abreast of current developments in the field of privacy law. It is not, however, to be used or relied upon as a substitute for professional advice. Before acting on any matter in the area, readers should discuss matters with their own professional advisers.