Submissions on Treasury Laws Amendment (Consumer Data Right) Bill 2018

By Simon Thompson
6 September 2018
simon.thompson15@gmail.com

I. Introduction

I am an Australian Lawyer and England and Wales qualified Solicitor. I have worked at technology and internet focused startups in London and Berlin. I have recently completed a Masters of E.U and transnational Information Technology and Intellectual Property law at University of Göttingen, Germany. I have completed a thesis titled Data Portability under the EU General Data Protection Regulation and Antitrust Law which focussed on the effects of the Right to Data Portability that exists at Art 20 EU General Data Protection Regulation ('GDPR') and the affects that it has on competition laws in relation to online platforms. I also hold a CIPP/E certification in European data privacy law. I have previously made submissions in relation to the ACCC's inquiry into online platforms.[1]

II. Preexisting World Standard for Data Portability - Art. 20 GDPR

There is already a world standard in existence for data portability.

The GDPR marks a shift in the way that the EU and the world views personal data and privacy. Building on its precursor, the Data Protection Directive, the GDPR has introduced, among other new concepts, the concept of data portability. Art. 20 GDPR gives data subjects the Right to Data Portability ('RtDP'), that is, data subjects have the right to receive the data that they have previously provided to a data controller in a structured, commonly used and machine readable format. Where technically feasible, this data is required to be transmitted directly between data controllers.

Art. 20 GDPR is set out as follows:

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

> the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
>
> the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

A. Origins and Development of the RtDP

The concept of the RtDP arose from data protection rights. In the EU data protection is seen as a fundamental right. Art. 7 European Charter for Fundamental Rights protects individuals from state interference in their private lives. Art. 8 of the European Charter for Fundamental Rights grants EU citizens the right to protection of their personal data, the right to fair and consensual processing of their data and the right of access to data and

[1] Copy available: https://www.accc.gov.au/system/files/Simon%20Thompson%20%28April%202018%29.pdf

rectification of that data. Art. 16(1) Treaty for the European Union grants EU citizens the right to the protection of their personal data.
In 1995 the EU adopted the Data Protection Directive, a milestone in the history of data protection.[2] On 25 January 2012 the EU Commission announced a proposal to reform and strengthen online privacy rights.[3] On 12 March 2014 the EU Parliament adopted the text of the GDPR. On 24 May 2016 the GDPR came into force. On 25 May 2018 the GDPR and the RtDP became enforceable.

Art. 14 Data Protection Directive gave data subjects a right to access their data and have it communicated to them in an intelligible format.[4] The GDPR maintains this right of access[5] and in addition gives data subjects a new right to access their data in a structured, commonly used and machine readable format. The RtDP also requires, where technically feasible, that the data subject shall have the right to transmit data directly from one data controller to another data controller.[6]

As can be seen, the EU has spent at least 7 years developing their current data protection law regime, including the RtDP.

In 2017 the EU considered building on the principles of the GDPR and extending data portability concepts to include machine generated data that does not fall within the scope of personal data as defined in the GDPR.[7]

B. Hindrance and Technical Feasibility

The RtDP requires that the data subject, once they receive their data, should be free to transmit that data without hindrance to another data controller. Where technically feasible the data subject has the right to have the data transmitted directly between data controllers.

The GDPR has also given rise to the Art 29 working party (now called the European Data Protection Board ('EDPB'), whose job is to opine of the implementation and interpretation of the GDPR.

Art 29 working party has given guidance on the term 'without hindrance', and has opined that:[8]

---

[2] "Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century." COM(2012) 9, December 25, 2012. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012DC0009&from=en., page. 3.

[3] "Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses." European Commission, January 25, 2012. http://europa.eu/rapid/press-release_IP-12-46_en.htm.

[4] Art. 12 Directive 95/46.

[5] Art. 15 Regulation 2016/679.

[6] Art. 20(2) *Ibid.*

[7] "Communication from the Commissions to the European Parliament, The Council, The European Economic and Social Commitee and the Committee of the Regions 'Building a European Data Economy.'" European Commission, January 10, 2017. https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy., page.15-16.

[8] Data Protection Working Party. "Guidelines on the Right to Data Portability." Directorate C (Fundamental rights and rule of law) of the European Commission, Directorate General Justice and Consumers, B-1049 Brussels, Belgium, Office No MO59 05/35, May 4, 2017. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233., page 15.

"Such hindrance can be characterised as any legal, technical or financial obstacles placed by data controller in order to refrain or slow down access, transmission or reuse by the data subject or by another data controller. For example, such hindrance could be: fees asked for delivering data, lack of interoperability or access to a data format or API or the provided format, excessive delay or complexity to retrieve the full dataset, deliberate obfuscation of the dataset, or specific and undue or excessive sectorial standardization or accreditation demands"

When clarifying the format of the data, the Art 29 working party then states:[9]

"Thus, portability aims to produce interoperable systems, not compatible systems"

When no common formats are used in a particular industry, the Art 29 working party states that data controllers should use open formats.[10] This requirement is still discretionary in nature, as it is not required that data controllers 'must use' open formats. It can be seen that the Art 29 working party has taken an expansive wide view of what 'without hinderance' means. The Art 29 working party has explicitly referred to the slowing down of access, transmission or reuse of the data however they have not gone as far as specifying that where possible, the transmission be spontaneous so as to facilitate, for example, real time cross platform messaging interoperability.
When determining what is meant by 'technically feasible', the Art 29 working party opines:[11]

"The technical feasibility of transmission from data controller to data controller, under the control of the data subject, should be assessed on a case by case basis."

There is no obligation on data controllers to develop, adopt or maintain processing systems which are technically compatible.[12] If direct transmission between data controllers is not possible, the Art 29 working party has equated this with a refusal to take action on a data subject request under Art 12(4)[13] and as such it must be explained to the data subject.

C. Classification of Data, Restrictions and IP

RtDP only applies to data concerning the data subject that the data subject has provided to the data controller by consenting to having the data processed, where the data was provided by the data subject so as to allow for the performance of a contract or where the data subject has requested that steps are taken prior to the entry into of a contract.[14] Personal data that is not processed by automated mean does not fall within the scope of the RtDP.[15] Personal data that was provided by the data subject for processing under lawful grounds such as 'legitimate interests' or other grounds set out at Art. 6 (1)(c)-(f) GDPR or Art. 9 (2)(b)-(j) GDPR is not retrievable under the RtDP.[16]

---

[9] [9] *Ibid.*, page. 17.

[10] *Ibid*., page. 19.

[11] *Ibid.,* page. 16.

[12] Recital 68 Regulation 2016/679.

[13] Data Protection Working Party. "Guidelines on the Right to Data Portability." Directorate C (Fundamental rights and rule of law) of the European Commission, Directorate General Justice and Consumers, B-1049 Brussels, Belgium, Office No MO59 05/35, May 4, 2017. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233., page. 16.

[14] Art. 20(1)(a) Regulation 2016/679.

[15] Art. 20(1)(b) *Ibid.*

[16] Recital 68 *Ibid.*

Some types or classifications of data are also not retrievable. The Art 29 working party has classified data into 3 distinct groups:[17]

> Data actively and knowingly provided by the data subject ('Actively Provided Data');
>
> Data that is observed by the data controller as a result of the data subjects use of the service ('Observed Data');
>
> Inferred data or derived data which is generated by the data controller as a result of the data subject's use of the service or algorithmic processing ('Inferred Data').

Actively Provided Data and Observed Data is data which is retrievable under the RtDP, whereas Inferred Data is not retrievable under the RtDP.[18]

The RtDP contains two exceptions to the ability to exercise the RtDP. These are when the retrieval of data interferes with a task carried out in the public interest or exercise of an official authority vested in the data controller and where the retrieval adversely affects the rights and freedoms of others.

Another exception is not specified in the GDPR but arises logically, that is, if the data controller has previously erased the data subjects data, the data controller cannot provide the data subject with their data because they do not have the data to provide.

Art 29 working party has opined that the 'preservation of rights and freedoms of others' referred to in the RtDP is to be interpreted as including trade secrets or intellectual property and in particular the copyright protecting software so as to to preserve the intellectual property rights of others.[19]

Art 29 working party also opines that a data portability request cannot be refused on the basis of an outstanding debt, contractual right or other trade conflict.[20] Where the data controller receives a request under the RtDP they cannot refuse on the grounds of possible business risk.

The WP29 has opined that the data controller could transmit the data subjects data in a manner that does not release information covered by trade secrets or other intellectual property rights.[21]

D. Enforcement and Penalties

Non compliance with the RtDP gives data subjects the right to lodge a complaint with a supervisory authority.[22]

Data subjects have the right to access a judicial remedy, without prejudice to any complaint that they may have lodged with a supervisory authority.[23] Third parties such as

---

[17] *Ibid*., page. 9.

[18] *Ibid*., page. 10.

[19] *Ibid.,* page. 12.

[20] *Ibid.,* page. 12.

[21] *Ibid.,* page. 12.

[22] Art 77 Regulation (EU) 2016/679.

[23] Art. 79 *Ibid.*

NGO's and consumer associations can also act on behalf of a data subject in the lodging of complaints or seeking of a judicial remedy where authorised by the data subject.[24] Penalties for non compliance with the RtDP are the higher of €20,000,000.00 or up to 4 % of the undertakings total worldwide annual turnover of the preceding financial year.[25] There is no opportunity for competitors of data controllers to lodge a complaint or seek judicial redress, so they lack any type of standing to enforce the RtDP and generally under the GDPR.

E. Other Sources of Data Portability

There are currently other sources of data portability rights in force or proposed. These are for example, Art. 13(2)(c) and Art. 16(4)(b) of the Proposed Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content. The EDPS has recommended that Art. 13 and 16 of the proposed Directive be aligned with the GDPR, this would also include the RtDP. The EDPS also recommends that if required, the measures be extended to include non personal data where required.[26]

Art. 36 Directive (EU) 2015/2366[27] on payment services in the internal market mandates the sharing of bank account data held by traditional financial institutions with payment institutions so that they can provide payment services that compete with those offered by the traditional financial institutions. This is in order to 'ensure fair competition between payment service providers'.

F. Conclusion on EU RtDP

As can be seen, the EU has already developed a robust, sophisticated and well drafted piece of legislation that facilitates data portability. It has already been translated into the languages of each EU member state and there is already a body of case law available that interprets key provisions of data privacy law in the EU. It is not clear why Australia is not mirroring the EU RtDP, especially since many Australian companies will be complying with the GDPR in any case.

III. Australian Businesses are already complying with the GDPR

Three out of four of Australia's largest financial institutions appear to be or at least are attempting to comply with the GDPR: Commonwealth Bank of Australia,[28] Westpac,[29] NAB[30] all appear to have GDPR privacy policies. As such they would also need to comply with the RtDP.

The proposed new Australian Consumer Data Right ('ACDR') will increase the regulatory burden for Australian businesses. In addition to complying with the worlds standard of

---

[24] Art. 80 *Ibid.*

[25] Art. 83(5) *Ibid.*

[26] "Opinion 4/2017 on the Proposal for a Directive on Certain Aspects Concerning Contracts for the Supply of Digital Content." Brussels: European Data Protection Supervisor, March 14, 2017. https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en.pdf, page. 19-20.

[27] Directive 2015/2366.

[28] https://www.commbank.com.au/content/dam/commbank/security-privacy/privacy-policy.pdf

[29] https://www.westpac.com.au/content/dam/public/wbc/documents/pdf/privacy/eu-data-protection-policy.pdf

[30] https://www.nab.com.au/content/dam/nabrwd/documents/policy/banking/eu-gdpr-privacy-statement.pdf

data portability, the RtDP contained in the GDPR, if the ACDR is allowed to proceed in its current format Australian business will have to also comply with an additional piece of legislation that will not provide consumers with additional privacy protections or any higher amount of data portability.

IV. Issues with specific parts of the Draft ACDR Bill

A. Section 56AA(b) - Access to data that is not 'reasonably identifiable'

In the GDPR, personal data is defined as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

In the ACDR, access is provided to third parties to consumers data that doesn't relate to 'identifiable or reasonably identifiable consumers'.

The problem with this section is that consumers will be identifiable by their data and people will be able to have access to this data. Also, what does 'reasonably identifiable 'mean? Does it mean data that has been protected by pseudonymisation, or anonymisation? When will an Australian Court give a judgement on this so the term actually has some meaning that will allow businesses to comply with it? There doesn't seem to be a large amount of judgements from Australian Courts on the Privacy Act and its interpretation, do the drafters of the ACDR expect that this term will be quickly litigated in a superior Court to allow for its proper definition?

This problem can be illustrated by the case of Patrick Breyer v Germany[31] involving Mr Breyer asserting that the German Government was holding data that was personal data because the government collected the IP address of people that accessed their websites. Even though the German government only had the IP address, because a third party internet service provider would have records of who was assigned the IP address, and these records could be used to identify the person behind the IP address, the IP address was held to be 'personal data' that was capable of identifying an individual.

Allowing data controllers to share data where it doesn't 'reasonably identify' a person will deter people from using the ACDR because consumers are not protected by a robust data protection regime that ensures their right to privacy. The data can be used and compiled to identify the individual that has provided it.

The ACDR is supposed to be a "Consumer Data Right". In effect it actually removes data privacy rights from consumers because it allows third parties to access they data in cases where the consumers can by identified. Consumers will not understand this and could make use of it to make switching easier, however consumers will pay a price in that third parties will have access to their data and they will be able to identify the consumers again be correlate of data from different sources.

B. Section 56AC - Ministerial Delegation and political influence

As a result of the ACDR being applied in a sector specific manner, this allows sectors to lobby against being subject to the ACDR. Those sectors that have achieved incumbency as a result of a lack of ability of consumers to multi home, as a result of high switching

[31] Patrick Breyer v Bundesrepublik Deutschland Case C-582/14 (ECJ) copy available at: http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN

costs, lock in effects and the subsequent network effects, these industries will attempt to exert large influence over ministerial decisions.

It is not entirely clear why the ACDR is not a blanket provision that applies to all consumers data, empowering consumers by giving them the ability to exercise informational self-determination over their personal data. The RtDP contained in the GDPR does this, why can't the ACDR?

C. Section 56AF(1) - Observed Data

As was seen from the implementation of the RtDP, data can be classified generally into three types, Actively Provided Data that the data subject actively gives to the data controller, Observed Data that the data subject generates as a result of the data subject using the services of the data controller (such as Spotify song lists or matches on matchmaking apps) and Derived Data that the data controller obtains as a result of processing the Actively Provided Data and Observed Data. The ACDR is silent on Observed Data as classified under the GDPR. Will the ACDR apply to Observed Data so as to allow consumers to easily port their data from music streaming services or matchmaking apps?

D. Section 56AF(4)(b) - Accreditation of data processors

There doesn't appear to be any delineation between data holders and data processors in the proposed ACDR bill. As is seen in the GDPR, a distinction needs to be made between the controllers of the data and those parties that are merely acting as the data controllers servants and performing processing.

It is not clear whether, for example, a third party doing data processing on behalf of a large bank would need to also become accredited under the ACDR accreditation scheme. If this is the case, this would involve thousands of third party data processors located around the world to become accredited.

E. Section 56BF - Accreditation

It is not clear why an accreditation scheme has even been included in the proposed ACDR. Would it not be easier to simply have a robust set of data privacy laws (such as the GDPR) and then prosecute data controllers and processors that do not comply with them? The threat of substantial fines (such as in the case of the GDPR, fines up to the higher of 20 million Euros or 4% of the firms world wide annual turnover) would mean that these parties would achieve compliance without the requirement for administration of a compliance system.

F. Section 56BM - Identification of consumers

The obligation to properly identify consumers before sending their data to a third party needs to fall on the data controller. For example, a criminal based outside of Australia who is attempting to obtain the personal data of an consumer by holding themselves out to a data controller as the consumer will not care about the possibility of being prosecuted in Australia for holding himself out as a consumer to which the ACDR applies. Australian criminal law is of no consequence to cyber criminals who live in, for example, Russia or Mauritius.

G. Section 56 EE - Option for pseudonymisation or non identification

Consumers will not understand the difference between full de-identification (such as by anonymisation) and partial, reversible de-identification that occurs via pseudonymisation. The data controller should not be able to offer the data subject a choice between these two options, full de-identification of consumer data (such as by anonymisation) should be required in all cases.

H. Section 56EI & 56EJ - Consent

The data rules do not yet exist and there doesn't appear to be any guidance on what consent would entail. What form would consent be required to be in, what needs to be included in the consent, how the consumer can actually consent to it and whether or not the consent needs to also include advice for the consumer (such as how to revoke the consent).

I. Protection of third party IP rights

There is no reference in the ACDR to the preservation of third party intellectual property rights. One can assume that the drafters did not intend for the ACDR to possibly destroy copyright, data base rights or other intellectual property rights such as trade secrets. Perhaps an exception to adverse affecting third party intellectual property rights needs to be included.

J. Protection of third party rights

A similar requirement to the protection of third party intellectual property rights is the requirement to protect the rights of other parties. Data controllers should not be able to transmit data to another data controller if it adversely affects a right of another party. Perhaps an exception to adversely affecting third party rights needs to be included.

V. Advancements of the GDPR Right to Data Portability

A. Consent of Minors

If Australia is intent on creating its own version of data portability law that doesn't conform with the GDPR and offers inferior protections for consumers, it should at least attempt to consider or remedy one of the problems with the GDPR, the obtaining of consent from minors. In the GDPR minors are deemed to be people that are aged under 16 years of age. This aged limit can be lowered to 13 in EU member state legislation of EU member countries. Problems are encountered where, for example a 15 year old would like to use an app that monitors health data, and provides health advice on fertility and contraception.

As the GDPR is currently drafted this would require that the parents or guardians of the 15 year old to provide consent to the 15 year old using the app. Two problems arise. The first is that there is no easy mechanism for businesses to actually verify that the 15 year olds parents or guardians have actually consented to the 15 year old using the app. The second, and more important is that there is a conflict between the rights fo the 15 year old to confidentially receive medical care or advice in relation to personal matters such as fertility or contraception and the obligation for companies to obtain the consent of the 15 years olds parents. If this consent is property obtained, it inherently means that the 15 year olds parents know that they are accessing an app related to fertility and contraception. A 15 year old should be able to freely access and share data about their health in order to receive medical advice. This is one downfall of the GDPR for which there is no easy solution. Perhaps a solution would be to provide an exception to the requirement for parental consent for the collection and sharing of very limited specific types of data related to health for minors, where the benefits of the collection and sharing of that health related data outweighs the potential harms to the minor. Perhaps this could be done on a company by company basis by way of application for exemption.

VI. Conclusion

Overall I am not supportive of the proposal.

The proposed laws are substandard when compared to the world standard of data portability (the EU GDPR), this law is already in existence and it is being complied with by many multinational firms. The GDPR has developed over several years and has gone

through rounds of consultation and refinement in Europe. Australia should simply mirror the provisions of the GDPR relating to the RtDP (Art 20 GDPR). This would give consumers better privacy protection and also allow for data sharing and easier compliance by businesses, because many businesses are already complying with the GDPR.