29 November 2020

Australian Attorney-General's Department
3-5 National Circuit, Barton
Canberra ACT 2600

Via Email: PrivacyActReview@ag.gov.au

Dear Sir/Madam,

Consultation — *Privacy Act Review*

illion (formerly Dun & Bradstreet Australia and New Zealand) is a data and analytics business we welcome the opportunity to provide this submission to the Attorney-General's Department in relation to the Privacy Act.

We have been in the data market in Australia for over 130 years and are also advancing new technology solutions by way of FinTech services such as Credit Simple (with over one million members in Australia) and illion Open Data Solutions (formerly Proviso), the leading aggregator of banking data in Australia. Both of these entities have recently been recognised by the ACCC as Accredited Data Recipients in relation to Open Banking (CDR)

illion's digital infrastructure is relied upon by over 15,000 corporate and government clients, and over 1.3 million consumers. It is vital that regulatory reforms satisfy consumer demands and continue to foster an environment that allows agility and innovation in data solutions.

General Comments

illion welcomes the government's decision to review the Privacy Act and is supportive of both the scope of the review and the consultative process that has been adopted.

We agree with the premise that a review is necessary as the digital economy has evolved to an extent that could not have been anticipated by the original Act and to an extent that means piecemeal amendments may not deliver the best outcome.

illion is also well aware of the inequality of the regulatory burden in relation to privacy. illion's businesses include a credit reporting body which is subject to highly specific regulation, CDR accredited businesses that are also subject to additional privacy safeguards and other businesses units that are subject only to the APPs. We recognise this is a result of historical attitudes to risk and the perception that banking and credit services are high risk. In our view other emerging businesses create new privacy risks which may not yet be subject to appropriate regulation. This review is an opportunity to address this.

illion is supportive of widening and clarifying the definition of personal information to include an individual's digital identity and footprint. We also support extending the requirements for consent gathering, and implementing a process for removal of consents. We note that the Consumer Data Right has already moved in this direction and an opportunity exists to create a single unified approach within the Privacy Act to avoid the possibility of greater inconsistency in information management.

We are also supportive of the creation of a right for individuals to seek direct redress for breaches of the Privacy Act in court, either through Direct Action or a Privacy Tort.

The only area of significant concern for illion is around changes to obligations around Third-Party Collection. Specifically, consideration of the practicalities of managing personal information in a compliant manner when the data is transferred to third parties, especially where new requirements such as consent management is considered.

Specific responses to questions for consideration where illion wish to make a response are included in the following section, illion's responses are in italics.

List of Questions for Consideration

Note: Responses are only provided for the subset of questions.

4. Should there be additional protections in relation to de-identified, anonymised and pseudonymised information? If so, what should these be?

illion is of the view that access to de-identified, anonymised and pseudonymised data is critical for the development and enhancement for products and services and delivers significant value to the Australian economy. We believe unnecessarily restricting this information will limit innovation and product development. While we welcome clarity on what is an acceptable deidentification process we believe that existing protections are adequate. We note that the adoption of industry standards could achieve this, such as the Data61 De-identification Decision-Making Framework.

We also recognise an uplift in security requirements for entities holding such information would mitigate risk of harms in re-identification.

20. Does notice help people to understand and manage their personal information?

illion agrees that there are significant challenges in ensuring individuals are adequately informed on how their information is used and that they consent to that use. The risk of "notification fatigue" is significant and unlikely to achieve its aim. While we suspect that there will be challenges in the creation of standard terms and or icons illion supports this proposal in an effort to simplify messaging.

23. Where an entity collects an individual's personal information and is unable to notify the individual of the collection, should additional requirements or limitations be placed on the use or disclosure of that information?

illion has significant concerns around the practicality of management of third-party collection. As a credit reporting body, illion is familiar with third party collection as CRBs have no direct relationship with borrowers and rely on credit providers to obtain consents and make notifications. This is an area where all participants are highly regulated, to reflect the risk associated with the nature of the information.

Imposing significant cost and burden on businesses where there may be significantly less privacy risk would be unjustified. We also note that in some case an expectation by the consumer would not require notification or limitations on use. In addition, if a statutory right of action were introduced, it would act as a deterrent to third party collectors to misuse information.

We note that the Consumer Data Right has to some extent considered the ability for individuals to be more specific on the use of their data, creating a complex consent model. The danger of this is that it is likely to further confuse consumers and become unmanageable across the range of entities where a consumer's information may be held.

25. Would a standardised framework of notice, such as standard words or icons, be effective in assisting consumers to understand how entities are using their personal information?

Standard phrasing and icons could be beneficial, and may address some of the challenges around consumer understanding.

26. Is consent an effective way for people to manage their personal information?

illion believes consent is critical, but there is a need to improve the clarity and purpose of consents.

27. What approaches should be considered to ensure that consent to the collection, use and disclosure of information is freely given and informed?

Greater transparency and standardised phrasing for use cases, although this can be challenging where innovation creates new use cases that have not been contemplated at the time consents are obtained.

Consumers have by their actions often demonstrated that either they understand the trade-off of consent for fee free goods and services, or that they have no interest in exploring the privacy issue.

By way of example we note consumers will often accept direct marketing in return for the services provided in an app on the basis that the service is provided free of charge or at a significant discount to the genuine costs that would have been otherwise possible.

28. Should individuals be required to separately consent to each purpose for which an entity collects, uses and discloses information? What would be the benefits or disadvantages of requiring individual consents for each primary purpose?

There is a need to avoid a very prescriptive approach, to allow for some flexibility and not prevent innovation, consent fatigue and to recognise that depersonalised data is exactly that "depersonalised" and required for research and development purposes.

There is also a danger that an overly prescriptive regime will introduce higher costs and complexity to providing commercially viable solutions (as the cost of compliance increases, and the permissible use of the data decreases). So, while the ultimate goal of protecting privacy is welcome, the price of achieving this is a reduction in innovative solutions being provided to consumers at low (or no) cost which may be to the ultimate detriment of the consumer.

The concept of legitimate interest in the GDPR as an alternative basis to processing personal information is one worth considering in light of the risks of notification fatigue.

29. Are the existing protections effective to stop the unnecessary collection of personal information? a. If an individual refuses to consent to their personal information being collected, used or disclosed for a purpose that is not necessary for providing the relevant product or service, should that be grounds to deny them access to that product or service?

Consideration must be given to the commercial model that is being used for the provision of a service. There has been a proliferation of services provided at no cost to the consumer on the basis that data that is made available.

If a user does not consent to the collection and use of data then the commercial model may no longer be viable, so restricting access to entire solutions, to certain functions within a solution, or introducing an additional charge where consent is not provided are all reasonable commercial responses should the data not be available for additional uses.

As noted above we maintain consent is critical and also encourage continued flexibility on uses to ensure this does not inhibit innovation and product development.

34. How can the personal information of individuals be protected where IoT devices collect personal information from multiple individuals?

It may be possible to address this challenge with better clarification on what is "personal" information given that devices are capturing data that is not currently recognised as "personal", while recognising the need to proceed with caution when expanding the definition of Personal Information.

38. Should entities be required to refresh an individual's consent on a regular basis? If so, how would this best be achieved?

There are dangers implicit in creating a requirement to refresh consent. We believe that refreshing consent is unnecessary and may prove unmanageable where large volumes of data are held, this is likely to lead to consumer frustration where entities constantly need to make contact to refresh their consents and will inevitably lead to notice / consent fatigue.

We note the current requirements for consent – voluntary, specific, informed and current mean that based on individual business circumstances the meaning of "current" relative to the products and services and ongoing commercial relationship may vary. Again, if there is a continuing commercial relationship the requirement to specifically refresh consent would appear redundant. The "legitimate interest" approach may be applicable here.

Consumer Data Right addresses this with the concept of consent being provided for a stated period of time, after which consent lapses and PI data has to be removed. This is a reasonable approach, although CDR also requires the creation of dashboards for consumers to manage their consent and recognises that depersonalisation changes the nature of the data completely.

We would encourage a mechanism that is simple to operate, to avoid creating consumer frustration and unnecessarily complex compliance obligations for industry. Any new proposal would also need to be simple for consent to be provided and maintained by an individual to avoid overwhelming them with requests to re-confirm consent.

In a risk context, the cost and complexity or refreshing consent as opposed to the risk is not one that appears to work at scale. Given that in any compliant marketing communication a consumer will have the ability to opt out, in the absence of opt outs there is an implied continuing consent.

44. Should there be greater requirements placed on entities to destroy or de-identify personal information that they hold?

In the current act this is a "principle" only and so does not prescribe requirements. Consequently, individual legislation is evolving with more prescriptive approaches, for example is the Consumer Data Right which is prescriptive about how long the information can be held for.

illion encourages a clearer approach in the Privacy Act, removing the need for inconsistent interpretations and avoid the risk of different approaches being introduced in relation to different data sets. While this is the case we maintain that depersonalised data should not be impacted by this.

The privacy risks in not destroying or de-identifying personal information are primarily misuse by the entity, or unauthorised access to that information by a third party i.e. a data breach. An uplift in

security requirements for entities holding such information would mitigate the risk of breach. Misuse is already addressed and would be strengthened by an individual right to action for privacy breach.

As noted above the adoption of industry standards such as the Data61 De-identification Decision-Making Framework could encourage uniform de identification practices.

45. Should amendments be made to the Act to enhance:
a. transparency to individuals about what personal information is being collected and used by entities?

illion suggest that additional clarity on what constitutes personal information, acceptable depersonalisation and therefore what is not personal information would be helpful.

b. the ability for personal information to be kept up to date or corrected?

In illion's experience the current Privacy Act already provides for the need for personal information to be kept up to date. There is also a need to balance concept of maintaining accurate records so that an update is not a correction and the retention of historic records remains valid (i.e. do not delete/destroy an old record) for audit / record keeping purposes.

48. What are the benefits and disadvantages of the current accountability approach to cross-border disclosures of personal information? a. Are APP 8 and section 16C still appropriately framed?

illion primarily provides solutions hosted in Australia. However, we have a limited number of solutions that we resell that do require Personal Information to be disclosed outside of Australia. In doing so we have first-hand experience of Australian entities working very hard to ensure that they have confidence that their obligations under the Australian Privacy Act are maintained irrespective of how or where the data is held.

This can prove very difficult, even when we are dealing with organisations in Europe who are meeting stringent standards such as GDPR. It is increasingly evident that large organisation who are compliant with the GDPR consider it to be the "gold standard" and are generally unwilling to make variations to terms for a small market such as Australia. Given the significant overlap, as set out in the comparison table published by the OAIC on 18 June 2018, it would be relevant to consider a carve out or other simplified treatment for data transfers with GDPR compliant entities.

We would therefore welcome a mechanism that more easily enables cross-border transfer for personal information where organisations are able to confirm that the data will be managed in a manner consistent with Australian legislation.

51. What would be the benefits of developing a domestic privacy certification scheme, in addition to implementing the CBPR system?

illion strongly supports a certification mechanism that provides confidence that suppliers are compliant with the legislation. This would reduce the time and effort illion currently has to expend to validate the capabilities of our suppliers while also providing a mechanism for us to demonstrate compliance to our customers.

illion recognises that many generally accepted industry standards such as ISO 27001 and others that are regularly used by GDPR regulated entities would be appropriate to form the basis of a certification so as to reduce cost burdens and streamline contractual compliance for businesses.

56. How should any direct right of action under the Act be framed so as to give individuals greater control over their personal information and provide additional incentive for APP entities to comply with their obligations while balancing the need to appropriately direct court resources?

As stated in the introduction illion is supportive of a mechanism for individuals to take direct legal action over failures to meet the obligations of the Privacy Act. illion does not have an opinion as to whether a Direct right of action of a Statutory Privacy Tort (or both) offers the best approach.

66. Should there continue to be separate privacy protections to address specific privacy risks and concerns?

illion provides services to multiple sectors of the economy, and across all States and Territories. There is a cost to compliance, and complying to varying obligations across different States and in different industry segments increases that cost while adding little benefit for consumers or Industry alike. For the sake of simplicity illion has a strong preference for a single Federal Privacy Act that is clear and prescriptive such that we avoid the need for additional more prescriptive legislation that applies to privacy.

As stated at the start of this submission, illion is also well aware of the inequality of the regulatory burden in relation to privacy. illion's businesses include a credit reporting body which is subject to highly specific regulation, CDR accredited businesses that are also subject to additional privacy safeguards and other businesses units that are subject only to the APPs. Our clients are domestic and international, including GDPR regulated entities and when we contract with state government agencies, they are subject to similar but different state regimes. Specific industries such as utilities, telcos and insurance clients are also subject to some overlap in privacy regulation.

Any harmonisation of privacy regulation which reduces overlapping regulatory burden will assist business compliance and consequently consumers.

68. Are the compliance obligations in certain sectors proportionate and appropriate to public expectations?

As noted, illion business units are subject to varying level of compliance obligations as a result of historical attitudes to risk and the perception that banking and credit services are high risk. In our view other emerging businesses create new privacy risks which may not yet be subject to appropriate regulation, and the public is increasingly demanding more from traditionally less regulated industries. This review provides an opportunity to address this issue as flagged in the final report for the Digital Platforms Inquiry in July 2019.

Conclusion

In conclusion, illion is supportive of this review occurring and the manner in which it is being undertaken. We welcome the opportunity to provide a submission and look forward to continued engagement through the process.