Summary of Privacy Roundtable Meeting

On 1 March 2019, the Australian Competition and Consumer Commission (**ACCC**) held an invitation-only roundtable meeting in Sydney. The purpose of the roundtable was to provide key stakeholders and representatives with an interest in privacy and data protection issues with an opportunity to discuss their views regarding the data and privacy-related key findings, preliminary recommendations and areas for further analysis identified in Chapter 5 of the ACCC's Digital Platforms Inquiry preliminary report.

The meeting was co-chaired by ACCC Deputy Chair Delia Rickard and Australian Information Commissioner and Privacy Commissioner Angelene Falk. Also in attendance was ACCC Chair Rod Sims and staff from the ACCC and the Office of the Australian Information Commissioner (**OAIC**). Key stakeholders in attendance included representatives of digital platforms, data brokers and analytics firms, privacy experts, consultants and advocates, consumer groups, and relevant Federal government agencies and departments.

The meeting agenda is **Attachment A.**

The following is a summary of the issues discussed at the roundtable meeting.

1. The objectives of privacy regulation and its potential impact on competition and consumers

The impact of privacy law on consumer protection in digital markets

Stakeholders discussed the role of privacy law within the context of digital markets and its impact on both consumers and businesses. Many stakeholders mentioned that transparency was an important factor in any notification and consent regime.

Some stakeholders noted that consent was only one important aspect of data protection and that other important aspects include the data minimisation principle and adequate regulatory oversight. A stakeholder proposed that adopting stricter definitions of both primary and secondary purposes for data collection would allow for better alignment with the data minimisation principle.

There were conflicting views on the effectiveness of data anonymization techniques, including de-identification, to protect consumer privacy. Some stakeholders observed that data governance, data security and privacy are all interconnected and are all important to the protection of consumer data, which could to some extent be strengthened by the development of a pro forma privacy policy to help build the security framework.

The importance of international co-operation and co-ordination

Some stakeholders expressed support of the EU's General Data Protection Regulation (**GDPR**).

Some stakeholders expressed favourable views regarding the GDPR as a level of privacy protection Australia should aim for, with one stakeholder describing it as the de facto global

standard. However, another stakeholder expressed the view that current Australian privacy law was not far removed from the privacy protections offered by the GDPR.

One stakeholder operating in multiple jurisdictions globally, noted that the different privacy laws across different countries posed a real and significant cost to their business. It was suggested that the harmonisation of privacy laws internationally is important to reducing costs to businesses and would also result in synergies that improved general compliance.

However, some stakeholders noted the high cost of compliance with the GDPR. One stakeholder also noted that the GDPR could benefit from some thoughtful exceptions. For example, the GDPR currently requires companies to re-identify data that had been de-identified for security or fraud reasons if an individual requests access. Other stakeholders noted that in their view, the ability to re-identify 'de-identified' data demonstrates that de-identification is not effective as a strategy to protect privacy.

A view was also put by a stakeholder that all the different Australian privacy related regulations and proposed reforms including the Consumer Data Right, Privacy Act, and proposed recommendations in the DPI preliminary report should be harmonised.

Some stakeholders supported the ACCC's preliminary recommendation regarding third-party audit and certification, suggesting such systems may provide a useful method to inform consumers about how their information is being treated by a business where their data has been transformed (by being value-added or used to create inferred information), without providing direct access to such value added or inferred data.

Another stakeholder noted that, whilst the GDPR was a great opportunity to remind consumers about their privacy controls, it should be considered whether the reminders and privacy updates are actually being read by consumers, noting that the lengths of many privacy policies had increased following the GDPR.

The impact of privacy laws on innovation in digital markets

Some noted the efforts of major digital platforms in collaborating to build a framework for allowing meaningful control of data for consumers.

Other stakeholders argued that it was important to demonstrate to consumers that the Australian Government is protecting people's personal information for it to encourage data-driven innovations within Australia. In particular, it was argued that there has been a steady reduction of trust in the digital economy which was increasingly impacting younger users from engaging with particularly technologies. It was also put that some digital economy developments which are increasingly impacting on consumer's lives, such as eScores, are still opaque in their operation and further that protecting personal and de-identified information is increasingly difficult with new technologies and analysis methods that may identify individuals (such as swipe recognition etc).

Recommendation 8(a) – strengthen notification requirements

What are the key elements of an effective notification scheme?

A number of stakeholders indicated that specificity is important in an effective notification, yet the level of specificity required varies between users. One stakeholder also noted that notification should not be viewed as establishing consent. Some stakeholders recommended a layered approach to presenting information in notifications, starting with a first layer of key information for users and a second layer with additional specific details for users who want to know more. A stakeholder noted that an effective notification should also involve a significant amount of consumer testing to ensure that consumers really do understand the disclosures

in practice. Some stakeholders argued that layered consents were already being used by some digital platforms.

One stakeholder recommended a standardised approach and requirements to ensure that information is presented not as marketing statements but as informative statements, similar to how nutritional information must be presented to consumers. This means that important information about the extent of collection, use and disclosure should be headlined, rather than general assurances of privacy protections. A stakeholder noted that the creative commons licence is an example of using a standardised legal document to convey complex legal obligations and rights.

Should similar disclosures be required of de-identified data?

Some stakeholders suggested that strong technical systems would help businesses meet privacy law requirements and considered that the use of de-identified user data should not require consent and notification of the consumer if it has been properly de-identified.

However, another stakeholder expressed concerns with the stability of de-identified data and noted the tendency for de-identification to degrade over time as new technologies are developed. Concerns were also raised with the risk of re-identification when datasets are combined. It was suggested that there should be certain rights and conditions regarding consumer's personal information that individuals cannot give away even where they have provided consent.

Another stakeholder supported the inclusion of de-identified data within proposed notification and consent requirements, particularly where de-identified data is being combined with other datasets, due to, it was argued, the significant opacity in how this information is dealt with and the resulting risks to consumers.

Recommendation 8(c) – strengthen notification requirements

Key elements of informed consent

Some stakeholders noted that there are situations where obtaining consent from consumers is not feasible and that consent also carries transaction costs. However some stakeholders also raised that consent can still be useful where it is possible to obtain true, informed consent from consumers. Other stakeholders noted that consent should be easy and it should be clear what a consumer is consenting to and that true consent should be assessed with regards to whether it is voluntary, truly informed, unbundled, revocable, before-the-fact, specific, limited, and fair.

Impact of consent fatigue

Some stakeholders argued that the ACCC's DPI Preliminary Report Preliminary Recommendation for consents (8(c)) – being that consent should ensure that they are unbundled and specific but without resulting in an impracticable number of consents that burden consumers- is contradictory, because in their view, obtaining the specific consent of consumers may burden consumers with an unmanageable amount of consents. One stakeholder emphasised the number of businesses which create data and suggested that consumers would be overwhelmed if the consents required were unbundled and specific.

Some also suggested that any consent regime should not stifle innovation, which was argued could occur if companies were expected to obtain new consents to use personal information for a slightly different purpose to the purpose for which the original consent was obtained.

However, other stakeholders cautioned against over simplification of consents and some companies' practice of seeking consent for a very broad primary purpose.

Best practice regarding seeking consent from children?

The current policies governing the creation of user accounts on digital platforms by children was discussed among stakeholders.

Some stakeholders noted that a number of digital platforms require children to be over the age of 13 before creating online accounts and have various parental controls and security systems in place to detect and report both underage and fraudulent accounts.

Some stakeholders noted that obtaining the age of users still required acceptance of a declaration of age, and guardian supervision/acceptance, at face value. Further, that if further age verification was required through the use of personal identification, for example, that this may conflict with over overarching data minimisation principles. Some argued that obtaining consents for persons under 13 does not work.

Area for further analysis: opt-in targeted advertising

Stakeholders discussed the potential impact of opt-in targeted advertising on businesses and it was noted that a range of online businesses, including media and other publishers, rely on the use of data to deliver targeted advertising on their platforms.

Some stakeholders noted that some digital platforms provide users in Australia with an option to opt-out of targeted advertising and suggested that the number of users who did opt-out was small. Another stakeholder considered this to indicate that requiring opt-in targeted advertising may not necessarily negatively impact digital platforms' business models.

One stakeholder expressed the view that existing opt-outs for cookie trackers on websites are dysfunctional and do not work. Another stakeholder maintained that providing consumers with the option to add targeted advertising provided using first-party data (data already provided to the digital platform through its use), will not necessarily address the privacy concerns associated with third-party data exchanges occurring in the ad-tech markets, which is complex and involves a large number of systems which tracks consumer's information in ways which they may be unaware.

Another stakeholder maintained that targeted advertising is both common and beneficial to businesses and there should be an economy wide discussion before any changes to targeting advertising are made.

Recommendation 8(d): enable the erasure of personal information

A number of stakeholders were supportive of this preliminary recommendation, however some stakeholders expressed concerns that consumer education in this area was still lacking.

Another stakeholder expressed concerns regarding the ability of this preliminary recommendation to address the opacity in the ad tech markets because the data remains in the digital space, even if it was deleted by the business who initially collected it, and in some cases the data can be used and on-sold to different businesses for different purposes.

Other stakeholders supported the preliminary recommendation to enable erasure of personal information and noted that it should be broadened to include data that is collected without consent and should include an ability for users to 'de-link' their data from a business, in a similar way to how the right to erasure operates under the GDPR.

One stakeholder suggested this preliminary recommendation is particularly relevant in relation to children's data.

Area for further analysis: mandatory deletion of user data

One stakeholder questioned whether consumers should be able to request the deletion of their data when the data carries economic value and was provided by users in exchange for use of a service. Another stakeholder noted that this may conflict with consumers' understanding of the transaction and should potentially be made clearer to consumers.

Some stakeholders suggested that this proposal could stifle business innovation and further noted concerns with consumers wanting to retrieve data after it has been deleted. Several stakeholders noted that they already had measures in place for users to delete their user data as part of their data minimisation policy.

Some stakeholders noted that there is a need to strike a balance between the types of data covered by a potential obligation to delete data and how businesses other than digital platforms may be affected by such an obligation across the economy. Some stakeholders expressed concerns that automatic deletion of data may not meet consumer expectations for certain services (such as email services etc).

Recommendations 8(e) and (f): Individual direct right of actions and increase in penalties

Stakeholders discussed whether the size of the penalty proposed by these preliminary recommendations were proportionate to the risk of harm.

Some stakeholders supported an increase to align with the GDPR penalties, whilst other stakeholders were concerned that increasing penalties may stifle innovation and could also incentivise businesses to cover up data breaches. It was suggested that recent changes to the Privacy Act (such as the mandatory data breach notification scheme) should be allowed to be take effect before a decision is made to introduce further changes such as individual causes of action and increased penalties.

Stakeholders further noted that the size of the penalty should be proportionate to the risk of harm to the consumer. Some suggested that the penalties should be at a level that they are not seen as a 'cost of doing business'.

Some stakeholders indicated support more generally for consumers to bring individual causes of action under the Privacy Act, noting that such rights are available to consumers under other regulation such as the Australian Consumer Law.

Some suggested the potential for an industry-led working group to cooperate with regulators on these issues and expressed concern with a move to rules based changes from the existing principles based framework. Others questioned the effectiveness of the existing principles based framework and non-binding guidelines issued by the OAIC.

Recommendation 9: OAIC Code of Practice for digital platforms

Stakeholders had varied views on the need for a code of practice administered by the OAIC. Some stakeholders were supportive of the recommendation if it extended beyond the current privacy framework and could operate at a higher standard than the Privacy Act.

Other stakeholders expressed concerns that having the Code of Practice apply only to digital platforms would not adequately address issues of lack of transparency, as this is an issue across many industries and markets. Another stakeholder noted that singling out certain industries added to the already complex privacy framework, which would confuse consumers

and deter business compliance. Some stakeholders suggested that this Code should therefore apply industry-wide.

Recommendation 10: Statutory cause of action for serious invasions of privacy

Some stakeholders were supportive of this recommendation, with a stakeholder noting that the proposed statutory tort should be in addition to the recommendation to introduce a direct right of action for individuals under the Privacy Act. Another stakeholder expressed the view that the scope of the action should include conduct that is negligent, as well as deliberate and reckless.

Additional Comments and Suggestions

Some stakeholders suggested that the definition of 'personal information' within the Australian Privacy Act should be examined and possibly amended, noting the differences in the definition of 'personal information' in Australian privacy law and in overseas privacy laws. Another stakeholder expressed the view that the current Australian privacy framework is robust and shares elements with the GDPR, but work needs to be done to address inconsistencies and gaps in the current Australian framework.

Another stakeholder expressed concerns that regulation of data collection may stifle innovation as the digital economy is reliant on data flows and that a balance should be maintained between consumer trust and sustaining innovation. Some suggested that where possible, technological fixes should be sought for privacy issues rather than regulatory changes alone. There was an emphasis by some on the need to ensure any system enables consumer trust and therefore the sustainability of the digital economy and innovation.

A number of stakeholders noted that many issues discussed could be mitigated with an increase in consumer education. Another stakeholder noted that consumer education was valuable as it influences consumer decision making, as consumers 'vote with their feet'. This affects businesses as they are deeply concerned with reputational damage, and see financial penalties as a cost of doing business.

However, other stakeholders suggested that focusing on consumer education alone is insufficient as businesses may engage in education only for the purposes of gaining the trust of consumers rather than informing consumers. It was suggested that any education initiatives developed need to account for the potential technological illiteracy of some consumers.

Attachment A – Privacy Roundtable agenda

8.45am – 9.00am	Registration
9.00am – 9.15am	Introduction, welcome and housekeeping
9.15am – 11.15am	**Session 1** discussion on: • Objectives of privacy regulation and its potential impacts on competition and consumers. • Preliminary recommendations and proposals in the areas for analysis identified in the DPI Preliminary Report on amendments to the Privacy Act to improve consent and notification processes: ○ **Recommendation 8(a)** – strengthen notification requirements ○ **Recommendation 8(c)** – strengthen consent requirements ○ **Recommendation 8(d)** – enable the erasure of personal information ○ **Matter for further analysis** – legislative requirement opt-in only targeted advertising ○ **Matter for further analysis** – requirement for automatic deletion of user data
11.15am – 11.45am	Break
11.45am – 12:45pm	**Session 2** discussion on other privacy related preliminary recommendations / proposals from the DPI Preliminary Report: • Other proposed amendments to the Privacy Act to enhance enforcement and deterrence ○ **Recommendation 8(b)** – independent third party certification ○ **Recommendation 8(e)** – increased penalties for breach of the Act ○ **Recommendation 8(f)** – direct rights of action for individuals ○ **Recommendation 8(g)** – expanded resourcing for the OAIC • **Recommendation 9** – OAIC code of practice for digital platforms. • **Recommendation 10** – statutory tort of serious invasions of privacy. • Additional comments and suggestions related to Privacy
12:45pm – 1:00pm	Concluding remarks