Response to the Privacy Act Review Report

March 2023

A. Introductory comments

Thank you for this opportunity to provide a submission to the Attorney-General's Department's Privacy Act Review Report (**Report**). The Department is to be commended on preparing a well thought out and comprehensive plan for the reform of Australia's Privacy Act 1988 (**Privacy Act**).

Oracle is a leading enterprise software company and cloud service provider. Oracle Advertising (**OA**, formerly known as Oracle Data Cloud) is a small line of business for Oracle and a rounding error for any Big Tech company. Yet OA's data brokerage business is subject to regulations that the largest digital platforms have skirted, despite their much more pervasive and damaging personal information collection practices. This is particularly true of Google and its parent company Alphabet, but also other global platforms, such as Meta and Amazon. Given the nature of its business, Oracle is well placed to comment in relation to amendments that are required to the Privacy Act to protect Australians in light of the realities of the personal information collection practices of these platforms (including Alphabet, Apple, Amazon, Meta, and Microsoft).

There is no doubt that the digital economy provides enormous benefits to consumers. This is true not only in Australia but internationally. However, there is a "dark side", where some digital platforms that dominate the provision of online consumer services (whether search, social media, e-retailing or other consumer services), collect vast quantities of personal information, significantly more than needed to deliver their services. Consumers have little visibility as to how much data is collected about them, or how their data is used or monetised. Further, consumers are not given meaningful choices related to data collection, with platform providers generally opting for a "take it or leave it" approach with consumers. Consumers typically must opt-out of data collection and, if overbroad consent is not given, products and services are not available.

The actions of the largest platforms — from their confusing and difficult to read "privacy" policies (which are in reality data collection policies), through to their intrusive and excessive personal information collection practices — have adversely impacted consumers and the Australian economy. Not only do the platforms collect unnecessary amounts of data from consumers, consumers do not and cannot know the true extent of the personal information collection they are "agreeing" to. Platforms are even less transparent about how consumers' personal information will be monetised and used. Personal information is made available through the monetisation practices of these platforms, not only to third-party advertisers but also to others, harming both adults and children.

The ways the platforms collect, use, and monetise personal information erodes Australians' trust in the digital economy and is inconsistent with the objectives of the Privacy Act. A key outcome of the reforms of the Privacy Act should be to address these practices.

Oracle has set out in this submission the further measures that should be incorporated in a reformed Privacy Act to ensure that, moving forward, the Act both protects Australians and allows for innovative uses of personal information in a way that promotes competition and economic growth.

B. Reform of the Privacy Act should be implemented quickly

There is an urgent need to reform the Privacy Act to provide protections to Australians in the face of the ever more intrusive data collection practices engaged in by digital platform behemoths such as Google.

The need for reform of Australia's Privacy Act was first highlighted in the Australian Competition and Consumer Commission's (**ACCC**) Digital Platforms Inquiry. The final report from that Inquiry,[1] released in 2019, noted that there is a substantial disconnect between how Australian consumers believe their data should be treated and how it is actually treated. The ACCC was concerned even then, some four years ago, that existing regulatory frameworks for the collection and use of personal information were insufficient to address the challenges of digitalisation and the practical realities of targeted advertising, which relies on the collection, and monetisation, of ever increasing volumes of highly personal information. This disconnect highlighted by the ACCC in 2019 has only worsened with the increased use of smart home devices (which the ACCC is now investigating in its September 2023 Digital Platforms Review). Reflecting global trends, the concerns of Australian consumers with how their personal information is used and monetised continue to grow.

The final report from the ACCC's Digital Advertising Services Inquiry (**Ad Tech Inquiry**), published in September 2021, also highlighted the abuses that arise from the collection and use of the personal information of Australians, making recommendations for clarity to be provided in privacy policies[2] and also proposing regulatory reforms to address the significant competition advantages that Google has, arising from the vast quantities of consumer data that it holds.[3]

Since 2019, only limited action has been taken to reform the Privacy Act. In late 2022, the Privacy Legislation Amendment (Enforcement and Other Measures) Act became law, providing for increased penalties to be payable for breaches of the Privacy Act. While the implementation of those reforms to the Privacy Act was an important step, more work needs to be done to ensure that the Privacy Act is fit for purpose and provides appropriate privacy protections to Australians in the context of the digital economy.

As ACCC Chair Gina Cass-Gottlieb recently commented, in the context of the broader reform of regulation of digital platforms in Australia (emphasis added):[4]

> *Decisive action will ensure Australians can enjoy the immense benefits provided by digital platforms along with necessary safeguards to minimise harms and encourage trust and confidence online. Improving the functioning of these markets also presents an opportunity to realise far-reaching benefits across the economy, given the increasing importance of digital platforms to Australian businesses of all sizes and types.*
>
> *Given the significant costs from inaction in terms of reduced innovation, choice, higher costs and lower quality,* ***the need to act is urgent****.*

While that comment from the ACCC Chair related to Australian competition and consumer law reforms, it is equally true in relation to reforms of the Privacy Act. Urgent action is required to

---

[1] Available here, see generally the discussion in Chapter 7.
[2] Recommendation 1 in the final report from the Ad Tech Inquiry, available here.
[3] Recommendation 3 in the final report from the Ad Tech Inquiry.
[4] Speech to the Opportunities and Challenges in the Digital Revolution Conference at Monash University, 17 March 2023, available here.

reform the Privacy Act, to ensure that the personal information of Australians is appropriately protected when they use the internet and online services. This is a necessary pre-condition to allow Australians to continue to enjoy the benefits provided by digital platforms and, like the other reforms the ACCC Chair mentioned in her speech, will assist in the promotion of innovation and choice for Australian consumers and improve competition, which will have broader economic benefits.

Without urgent reform, the egregious behaviour of Google and other digital platforms which Australians cannot avoid in their daily lives and online interactions will continue. The underlying philosophy of the Privacy Act is "privacy by design". Google, one of the largest digital platforms which provides a plethora of online services to Australians, has a business model that is the antithesis of this. Google's business model is built on unfair, unrepentant and unrestrained data collection that no reasonable consumer can avoid. As the ACCC Chair has pointed out, competition and consumer protection law reforms are required to address these behaviours. However, equally, these behaviours should be addressed through reforms of the Privacy Act.

C. Definitions: personal information; targeting, trading and disclosure

1. Personal information definition requires further updating

The definition of personal information in the Privacy Act should be updated to reflect the various ways new products and services create, collect, and process data that is intimately tied to a consumer.

Traditional definitions of personal information include a consumer's name, government identifiers such as tax file number, and commercial identifiers such as an email address. Expanding the definition of personal information in the Privacy Act to include data that is uniquely and intimately tied to an individual consumer – for example their precise geolocation data, is an essential privacy protection for modern life. Additionally, unique electronic identifiers such as a smartphone's IMEI or an account identifier should be recognised as equally as sensitive as email addresses, because they can identify an individual and/or their devices.

Proposal 4.2 in the Report, which is that a non-exhaustive list of information which may be personal information should be included in the Privacy Act to assist those entities regulated by the Act (APP entities) to identify the types of information which could fall within the definition, is an appropriate reform for the Privacy Act.

In relation to proposal 4.2, the list of categories of personal information included in the Privacy Act should not be a prescriptive list, as the categories of personal information that digital platforms will collect over time will continue to evolve. The definition of personal information should be sufficiently broad and flexible to encompass those different categories, without express amendments being required to the Privacy Act. At the same time, the following points are very important:

(a) The Report refers to identification numbers and online identifiers. It should be clear that these include unique electronic identifiers such as a smartphone's IMEI or an account identifier. These identifiers are more important than a person's name – significant amounts of information may be linked to such identifiers that uniquely identify an individual, even if that individual's name is not known.

(b) We have commented on location data later in this submission. Location data, of itself, should be considered to be personal information under the reformed Privacy Act. It is also important that, as is intended under the Privacy Act reforms, personal information *inferred* from location data falls within the remit of the Privacy Act. Even "coarse" location data

revealing, for example, that an individual is within a certain city, might not of itself be sensitive personal information but could be used to infer sensitive personal information. The Privacy Act should therefore also include an acknowledgement that inferred information may be sensitive information, even if the source or sources used to make the inference are not.

2. **Definitions of "targeting", "trading" and "disclosure"**

The definitions of "targeting", "trading" and "disclosure" for the purposes of the Privacy Act must recognise the manner in which digital platforms monetise the personal information they collect.

Proposal 20.1 specifies that definitions of "targeting" and "trading" should be included in the Privacy Act:

(a) targeting would capture the collection, use and *disclosure* of information for the purposes of, amongst other matters, tailoring advertising provided to an individual, either on their own or as members of a group or class; and

(b) trading would capture the *disclosure* of personal information for a benefit, service or advantage.

These defined terms are then used in various other proposals in Chapter 20 of the Report, primarily the restrictions imposed in relation to targeting (proposals 20.3 and 20.6) and trading personal information (proposals 20.4 and 20.7).

The definitions of targeting and trading use the term "*disclosure*". Disclosure is not defined in the Privacy Act. The Office of the Australian Information Commissioner (**OAIC**) takes the view that an APP entity discloses personal information when it makes it accessible or visible to others outside the entity and releases the subsequent handling of the personal information from its effective control.[5] This very narrow and limited definition does not address the manner in which large digital platforms deal with the vast quantities of personal information that they collect and share with advertisers.

Google and Meta – companies that generate nearly all their revenue from advertising – proudly claim they do not ***sell*** consumer data, but how then do they make money? Advertising-dependent companies like Google and Meta are built on business models that depend on the collection of personal information across their products and services to sell targeted ads, though, at least in the case of Google, it does not actually *disclose* that personal information to third parties. To retain market power, these advertising companies serve as brokers to consumers' personal information, matching buyers of advertisements with consumers that meet advertisers' specific requirements. For example, Google and Meta match advertisers with consumers who are currently in a specific location, or are similar to current customers.

While consumers' personal information is not directly *disclosed* to an advertiser, within the meaning given to that term by the OAIC, it is shared and monetised – to the tune of $100s of billions of dollars each year. This method of personal information sharing and monetisation should be included in a new definition of *disclose* under the Privacy Act to ensure consumers are protected from abuses related to the unfettered and uncontrolled use of their personal information. Without incorporating in the Privacy Act a definition of disclose that includes these

[5] Paragraph B.64 of the OAIC's APP Guidelines.

activities of digital platforms, the proposals in Chapter 20 of the Report that relate to trading of personal information and restrictions on targeting, including proposals requiring consent to be obtained before an individual's personal information may be traded, and the prohibition on trading in the personal information of children, will not have the intended impact.

Further, to give full effect to the Chapter 20 reforms, section 13B of the Privacy Act should be repealed. That section currently allows an organisation that is a body corporate to collect personal information (other than sensitive information) from a related body corporate and, correspondingly, to disclose such personal information to a related body corporate without, in either case, a breach of the Privacy Act occurring. There is no practical benefit in allowing that exemption from the operation of the Privacy Act to continue. Where there is disclosure of any personal information between related bodies corporate, the proposed new provisions set out in Chapter 20, particularly in relation to trading, should apply.

D. Tracking must always require consent: proposal 4.10

The proposed definition of precise geolocation data must be modified to ensure that the definition of personal information includes the highly sensitive data of individuals that digital platforms such as Google collect as a result of their intrusive tracking practices.

1. **Narrow scope of proposal**

Proposal 4.10, to recognise that the collection, use, monetisation and storage of precise geolocation tracking data over time requires the consent of the individuals that are tracked, is supported. In this context "geolocation tracking data" will be defined as personal information which shows an individual's precise geolocation and that is collected and stored by reference to a particular individual at a particular place and time and tracked over time.

However, the current formulation of the definition of "geolocation tracking data", and the terms of proposal 4.10 more broadly, will mean that the outcomes intended by the Government from introducing proposal 4.10 in the Privacy Act will not be achieved. An explanation of the issues, and suggested resolutions, are outlined below.

2. **"by reference to a particular individual"**

It is unclear what is meant by the requirement in proposal 4.10 that the information is stored "by reference to a particular individual". As noted above, identifiers like a smartphone's IMEI are more important than a person's name. Where location data is collected over time and stored with any form of identifier, then that should be sufficient to satisfy the requirements of the new definition of precise geolocation data and to require consent to be obtained. In other words, it should not be necessary for the precise geolocation data to be stored by reference to the *name* of an individual. This should be made clear in the amendments made to the Privacy Act.

3. **"at particular places and times"**

It is not clear what the reference in proposal 4.10 to "at particular places and times" means. While proposal 4.10 need not include incidental limited uses of location data, such as to determine a person is in Australia so that the correct version of a website may be shown, this is addressed in the proposal by referring to tracking over time. If an individual's precise geolocation is collected, this should be sufficient for the proposed consent regime to apply. There should not

be an additional requirement that the geolocation data is linked to "at particular places and times".

4. **"and stored"**

When proposal 4.10 is incorporated in the Privacy Act, it should be clear that the individual's precise geolocation does not need to be both collected "and stored". Stored is not a defined term under the Privacy Act. "Collect" is defined in section 6 as (so far as is relevant here) collection for the purpose of inclusion in a record. It should therefore be sufficient that the geolocation data is *collected* for the proposed consent regime to apply.

Further, the Privacy Act should provide that the record in which the location data is included does not need to be held by the entity that initially facilitates the collection. For example, if one entity in a corporate group facilitates the collection and another entity actually includes that data in a record, the new regime should apply.

5. **Right to withhold consent should be unqualified**

Proposals 20.2 and 20.3 refer to an "unqualified right" to opt-out of personal information being used or monetised for direct marketing or targeting. We have discussed those proposals later in this submission, however there is one important point that those proposals address but that is not addressed in proposal 4.10. While 4.10 gives consumers the right to withhold their consent to the collection of their precise geolocation data, this is not stated to be an "unqualified right". When implemented, it should be clear that the right is unqualified – in the same way that the rights under proposals 20.2 and 20.3 are unqualified. In other words, if consent is not given by an individual, the individual should still be able to access the relevant products or services provided by the collecting entity (and any entity facilitating the collection).

6. **Expansion to other data that the largest platforms track**

The Report comments, though this is not included in the recommendation, that as part of implementing proposal 4.10 further consideration could be given to expanding location tracking data to other tracking metrics such as health data, heart rate and sleeping schedule. It is appropriate to consider the expansion of this proposal to circumstances where this type of data is tracked through consumer facing services for the purposes of targeting individuals with advertising, content or other similar consumer services. The largest digital platforms are continuing to move into markets for the provision of health services and therefore are also moving to tracking more and more health related data. Like location data, this is highly personal and can also be used to infer highly sensitive information about individuals. Accordingly, when collected by those platforms for advertising or similar purposes, this data should be treated in the same way as precise geolocation data.

7. **Right to request deletion is equally important**

We have commented later in this submission that not only should individuals have express consent rights for the collection of their geolocation data, but the proposed right of erasure (proposal 18.3) should allow individuals to require the deletion of all of this data.

Most importantly, "delete" should mean delete – not "retained in anonymized form" as Google purports to do.[6] As outlined in paragraph E.3 below, there is some personal information which simply cannot be anonymised, such as geolocation data, and the Privacy Act should be very clear

[6] https://policies.google.com/privacy?hl=en-US ("When you delete data, we follow a deletion process to make sure that your data is safely and completely removed from our servers ***or retained only in anonymized form***.") (emphasis added).

that a request for deletion should not allow personal information to be retained in any form, including a de-identified or anonymised form.

E. Clear information should be provided to consumers

1. Privacy policies should be correctly labelled

Privacy policies are data collection policies. To foster transparency, the Privacy Act should require that these policies are correctly named.

As is acknowledged in the Report,[7] "privacy policies" have the potential to play a crucial role in fostering transparency regarding the personal information handling practices of regulated entities. For that reason, the proposals in Chapter 10 of the Report should be amended to require that privacy policies should be renamed as *data collection policies*.

Continuing to name these policies as "privacy" policies is a misnomer that causes unnecessary consumer confusion and unrealistic expectations. The terms and conditions in these policies do not perform the role of outlining consumers' privacy rights. Rather, "privacy" policies instead include, as mandated by the Privacy Act, information about the rights of entities to collect, use and monetise the personal information of consumers. The simple act of correctly naming these policies for what they are – **data collection policies** – will ensure that even consumers who do not read the legalese that is included in such policies (notwithstanding the requirement of the Privacy Act that such policies should be "clearly expressed") intuitively understand the true nature and relationship of their agreement. This would go a long way towards ensuring that consumers are aware that their personal information is being collected and that they should read further if they wish to discover the exact nature of the personal information that is collected and how it is used and monetised.

Such a requirement would supplement the changes that are proposed to be made to Australian Privacy Principle (**APP**) 5 collection notices, as set out in chapter 10 of the Report, including proposal 10.1, which is that those collection notices should be clear, up-to-date, concise and understandable.

2. The ability of regulated entities to make changes to data collection policies should also be limited

Individuals should not be subject to amendments to "privacy" policies which they have not agreed.

The Report appears to assume that it is appropriate for APP entities to have an unfettered right to amend their "privacy" policies. For example, the Report refers to the OAIC's APP Guidelines, which state that "(a)n APP entity should regularly review and update its privacy policy to ensure that it reflects the entity's information handling practices, such as part of an entity's annual planning processes".[8]

The Privacy Act should recognise that these policies are, in fact, agreements between an APP entity and their customers or, in an online context, the users of their online services. As such,

[7] Chapter 10.

[8] Page 94 of the Report.

these should be considered to be contracts within the unfair contract terms regime of the Australian Consumer Law. Under the Australian Consumer Law a contract term is unfair if it:

(a) gives one party a significant advantage over the other;

(b) is not necessary to protect the legitimate interests of the dominant party to the contract (in the case of a privacy policy, the APP entity); and

(c) would cause financial or other harm to the party if enforced.

Providing an unfettered ability for each APP entity to amend its privacy policy is clearly unfair to consumers. It provides an advantage to the APP entity, as it allows it to significantly expand the circumstances in which it can use, disclose or monetise the personal information of a consumer, without that consumer having any rights to limit this; is not necessary to protect the interests of the APP entity, who should only use, disclose or monetise the personal information for the purposes disclosed and agreed when the information was provided; and, when a policy is changed, this would have an adverse impact on the consumer, who would not be able to object to new uses, disclosure or monetisation of their personal information that had already been collected, even if those purposes are not agreed by the consumer. Accordingly, this unfettered ability to amend privacy policies should be prohibited and void.

Consumers have a valid reliance interest in relation to the privacy policy that is in place when their personal information is first collected from an APP entity – they are rightfully entitled rely on the terms which they originally agreed with the APP entity regarding their personal information. Where a privacy policy is changed after personal information is first collected, a consumer (even if they are aware of the change, noting that there is no obligation imposed under the Privacy Act for an APP entity to notify consumers) is left with no meaningful choice – either they agree to the new terms, or stop using the products or services provided by the APP entity completely. Even if they stop using the products and services, the APP entity will be able to continue to use personal information already collected under the terms of the updated policy.

Accordingly, the unfair contract terms provisions of the Australian Consumer Law should be amended to expressly provide that unilateral changes to privacy policies are prohibited and void unless agreed by consumers. Consumers should be treated fairly and have meaningful ability to grant or withhold consent if an APP entity materially changes its personal information collection and management practices. The Privacy Act, in turn, should recognise that such unilateral changes are prohibited and void under the Australian Consumer Law.

3. Delete should mean delete

Proposal 18.3 is that, for the first time under Australia's privacy laws, individuals should have a right to require that an APP entity will delete the personal information that the APP entity holds about them.

This right should go further than currently proposed in the Report in relation to "large digital platforms". "Large digital platforms" should be defined as any digital platform that is subject to a code implemented under the new laws that are proposed to be put in place by the Government in response to the fifth report issued by the ACCC under its 5-year Digital Platform Services Inquiry.[9] This would include, at a minimum, Google and its parent company Alphabet, Amazon and Meta. Such a requirement could be included in a code made under the Privacy Act, as suggested in relation to consent rights in section F below.

[9] Available here.

An individual should have the right to require any large digital platforms to delete all of the individual's data that the platform has collected or monetised, including that which has been de-identified or is, to use the expression used in the Report, data that is otherwise considered to be "unidentified information", collected through tracking and the like.

In this context, and noting Oracle's separate comments in this submission in relation to precise geolocation data, that type of data in particular should fall within the scope of this regime, because it cannot be anonymised – as researchers have long recognised. Large digital platforms should be obligated to link precise geolocation data to a unique identifier for an individual, increasing accountability and permitting consumers who choose to delete their information under the proposed new right of erasure to do so completely.

F. Opt-in should always be the default for digital platforms

As the largest digital platforms are incentivised to collect as much personal information about their users as possible, opt-ins should always be the default for those platforms.

The Report has not recommended that consent is required to be obtained for the collection of personal information. The primary reason for this, as has been highlighted in the Report, arises from concerns that requirements to obtain consent in all circumstances where personal information is collected, used and disclosed (or monetised) may result in consent fatigue.

Nonetheless, there remains a case for consent, or opt-ins, to be mandated in the case of digital platforms such as Google and Meta, as well as other platforms that depend on monetising personal information to fund their products and services. These platforms are incentivised to abuse opt-out mechanisms to the detriment of consumers, privacy, and the marketplace as a whole. Opt-in data collection is the only way to ensure consumers have rights, confidence, and control over who has access to their personal information. Consumers should start with privacy as the default, and have the affirmative right to opt-in to the collection, sale, and monetisation of their personal information.

As would apply in the cases of Oracle's recommended change to proposal 18.3, the consent requirement would apply only to "large digital platforms", that is, any digital platform that is subject to a code that is implemented under the new laws that are proposed to be put in place by the Government in response to the fifth report issued by the ACCC under its 5-year Digital Platform Services Inquiry. If consent is required for any collection, use, disclosure or monetisation of any personal information only in these limited cases this will avoid the consent fatigue concerns that are raised in the Report. As only a limited number of digital platforms will be required to obtain such consents, this requirement will also assist in making clear to individuals that these platforms collect, as well as use and monetise, extensive amounts of personal information.

As for other consents under the Privacy Act, this should be an "unqualified" right. In other words, the code should provide that if consent is not given, the digital platform must continue to provide its products and services to the relevant individual.

Proposal 5.1 is that the Privacy Act should be amended to give power to the Information Commissioner to make an APP code in certain circumstances. This proposal should be expanded so that it requires a code to be developed for digital platforms that met relevant criteria. Such a code would be an appropriate means to be used give effect to the recommendation in this paragraph F.

G. Necessary protections for children

Improvements and updates to the Privacy Act that protect teens and children from deceptive online ads and digital manipulation are long overdue.

To protect the online privacy of teens and children, further changes to the proposals in both chapter 16 and chapter 20 of the Report are required. Specifically:

(a) *Capacity to consent:* Proposal 16.2, which would allow APP entities to determine whether an child under the age of 18 has the capacity to consent on a case-by-case basis and to generally rely on an assumption that children over 15 have capacity, should be deleted. This should be replaced by a proposal that requires APP entities to assume that any child under the age of 18 does *not* have the capacity to consent. Digital platforms, but also other APP entities, have an incentive to assume that children have capacity to provide consent to their exploitative personal information collection and management practices. To avoid such exploitation, parental or guardian consent should be required to be obtained for *all* children.

(b) *Direct marketing and targeting:* Proposal 20.5 is that direct marketing to a child is prohibited unless the personal information used for direct marketing was collected directly from the child and the direct marketing is in the child's best interests. Proposal 20.6 is that targeting of any child is prohibited unless it is in the child's best interests. The Report provides that "best interests" will not be defined.

Reference is made in the Report to, for example, the UK Age Appropriate Design Code and that, in the context of privacy law, determining whether a particular collection, use or disclosure is in the best interests of a child requires that the child's physical, psychological and emotional wellbeing is protected. It is not practicable to leave questions of "best interests" to be determined by digital platforms (or, for that matter, other APP entities). Without definition, this will always be a very subjective assessment, where APP entities will again be incentivised to determine that their particular collection, use, disclosure or monetisation of the personal information of children is in the best interests of those children.

The only practical way to provide protection would be to directly ban both direct marketing and targeted advertising to any child, which is the approach it is recommended the Australian Government adopts.

In any event, there will need to be very clear permissions in the Privacy Act to ensure that some forms of targeting to children are permitted, for example:

(i) where the targeting is to ensure compliance with laws, such as those that require that children may view only age appropriate content, or to allow for the operation of the Online Safety Act protections for children; and

(ii) for Government public service or health messaging, such as suicide prevention or similar.

The ability to lawfully provide these types of valuable and appropriate targeting services should not rely on a vague definition of "best interests".

H. Data portability

Australia should use its world class CDR regime to empower consumers and promote competition and innovation across the markets for different digital platforms services.

The Report briefly refers to the consumer data right (**CDR**) regime. That innovative regime, which is a world first in terms of its potential application across all sectors of the economy, has the potential to provide significant benefits to the Australian economy and all Australians.

The application of the CDR across different digital platforms services would be empowering for consumers. This would give consumers the ability to choose their technology partners in return for real value, rather than allowing only one platform, or a small number of platforms, to harvest and monetise an individual's personal information. At the same time, this would incentivise businesses to develop innovative ways to meet consumer needs and craft "privacy" policies to which consumers would actually consent. The broad roll out of the CDR regime would return power to the consumer and allow the free market to decide the winners of the digital economy.

This view is supported by the work of Australia's Productivity Commission. In mid-March the Productivity Commission released a nine volume report on Advancing Prosperity in Australia.[10] Volume 4 of that report addressed Australia's data and digital dividend. In relation to data collected by the private sector and the CDR, the Productivity Commission concluded that there is still much work to be done. It stated:[11]

> *The potential to use this data to improve decision making, tailor services for customers and generate operational efficiencies is now well established. Governments can support greater sharing and use of consumer data through data portability policies, enabling consumers to authorise businesses holding their data to provide that data to third parties.*

The reformed Privacy Act should acknowledge the benefits that the CDR has the potential to provide, and expressly acknowledge that the CDR enables the beneficial sharing and use of personal information where the consumer is truly in control of their own information.

I. Appropriate penalties

Fines shouldn't be just the cost of doing business. The OAIC and the courts should have the power to impose innovative remedies that provide for the reform of the egregious data practices of the largest platforms.

Monetary penalties do not work to hold the largest digital platforms accountable. These platforms are so profitable that an eventual monetary penalty is baked into their business models: it is just a cost of doing business. Innovative remedies for breaches of privacy and other laws are required to truly hold these platforms to account.

Proposal 25.5 in the Report is to amend sections 52(1)(b)(ii) and 52(1A)(c) of the Privacy Act. Those sections provide that, after undertaking an investigation under the Act, the Commissioner may make a declaration that the relevant person must perform any reasonable act or course of conduct to redress any loss or damage suffered by the impacted complainant or complainants.

---

[10] Available here.

[11] Page 48 of volume 4.

Proposal 25.5 is that these provisions should be expanded to require the relevant APP entity to identify, mitigate and redress any actual or reasonably foreseeable loss or damage suffered.

Proposal 25.5 should take further steps. Proposal 26.1 is that the Privacy Act should allow for a direct right of action to permit individuals to apply to the courts in relation to any breach of the Privacy Act that impacts them. An element of this right is that, in any such case, the court should be able to make *any order as the court sees fit*. An equivalent power should be given to the Commissioner under the Privacy Act.

In other words, if the Commissioner undertakes an investigation, as a result of receiving a complaint or on her own initiative, and finds that a breach of the Privacy Act has occurred, the Commissioner should have broader powers to order remedies that would truly provide redress. The Commissioner should have the power to require remedies that ensure the relevant practices cannot be continued in future, so that other individuals are not subject to the same problematic practices. If a greater range of remedies could be ordered by both the Commissioner and the courts, this would ensure that the largest digital platforms seriously considered their obligations under the Privacy Act.

Similar changes should be made in relation to section 13G of the Privacy Act. That section enables the Privacy Commissioner to commence legal proceedings for breaches of the Privacy Act. The only remedies that may be obtained are civil penalties. This section should be amended to allow for the Commissioner to seek, and the court to grant, any order as is necessary to provide redress for the relevant breach. This should not be limited to monetary fines.

J. Linkages between personal information collection practices and anti-competitive conduct require coordinated responses

There is an undeniable link between the personal information collection practices of the largest digital platforms and their anti-competitive behaviour.

This is clearly demonstrated by considering the case of Google and its dominant position in the ad tech services markets. Google's dominant position across a range of consumer facing digital services means that Google is able to impose unfair terms on individuals in relation to Google's personal information collection, use and monetisation practices through its privacy policy and terms of service. Consumers have little choice but to agree to these terms. As it is able to impose these unfair terms, Google collects vast quantities of personal information through Android OS and its consumer facing services. Google also collects consumer data through its ad tech services as, through these services, Google obtains data about how consumers interact with ads, which is data about a consumer's interests and preferences.

Personal information plays a crucial role in the provision of ad tech services. Google's unrivalled data position creates network effects in the form of a feedback loop in ad tech services markets. The more robust Google's consumer data pool is, the better Google's ad targeting becomes, and the more advertisers are driven to Google's ad tech services. Google's dominant position in the ad tech services markets has, in turn, allowed it to engage in many of the different types of anti-competitive conduct that the ACCC identified in the final report from its Ad Tech Inquiry.

The ACCC is not the only regulator to have called out the anti-competitive actions of Google in the ad tech services markets. For example, the US Department of Justice (**DOJ**), supported by seven US States and the Commonwealth of Virginia, has very recently commenced proceedings against

Google in relation to its anti-competitive practices in the ad tech services sector that have been facilitated by the vast quantities of personal information that Google holds.[12]

These examples demonstrates why the personal information collection practices of dominant digital platforms, which also cause significant harm to Australians who lose control of their own information, must be addressed consistently across both the reforms to the Privacy Act and in the proposed digital platforms regulation recommended by the ACCC which The Treasury has recently consulted on.[13] Without the adoption of a consistent approach to the regulation of the largest digital platforms, neither the new digital platforms regulation nor the Privacy Act reforms will have the intended positive outcomes of providing more control to individuals over their personal information and promoting competition and innovation in online markets.

Thank you for considering this submission. Oracle would be very happy to discuss any of the issues that we have raised with the Attorney-General's Department.

March 2023

ORACLE

[12] The DOJ's media release announcing these proceedings is available here.
[13] See here.