ORACLE CORPORATION

SUBMISSION TO THE INQUIRY INTO FUTURE DIRECTIONS FOR THE CONSUMER DATA RIGHT

10 JUNE 2020

Introduction

1. Thank you very much for providing an opportunity to Oracle Corporation (**Oracle**) to make this submission to The Treasury's Inquiry into Future Directions for the Consumer Data Right Inquiry (**Inquiry**).

2. Oracle is a global technology company with a broad portfolio of solutions for companies of all sizes. Oracle brings a unique perspective to the Inquiry in this submission, as its technology expertise means that it is well placed to comment in relation to the application of Australia's consumer data right (**CDR**) in the digital context.

3. The key intent of the Inquiry is to look at how the CDR could be enhanced to boost innovation and competition, and support the development of a safe and efficient digital economy, benefiting Australians and Australia. As Oracle explains in this submission, a key way to achieve those outcomes is to expand the CDR to enable the regime to be effectively applied to personal information which is collected from consumers when they use digital services, where those digital services are provided by digital platforms, via applications (**apps**) or from the use of a myriad of different internet connected devices, such as smart phones, smart TVs, smart speakers and the like.

4. A key type of information collected online is location data collected via mobile smart devices. Location data encompasses personal location and activity information which is collected from a consumer via her mobile device. That data may be collected from sensors such as GPS, WiFi, Bluetooth, etc. There are significant benefits in applying the CDR to location data, though potentially in future the CDR could be applied to other types of clearly defined digital personal information that is collected from consumers as they use digital services.

5. The location data collected by entities such as Google is very valuable. Consumers create that information and therefore own it. In recognition of this, consumers should have the right to share in the value of their location data and the right to have a greater choice and say in how that information is used. The CDR is able to be applied to grant consumers these rights.

> ***Applying the CDR to location data will provide consumers with control over this type of personal information in a way that has not been possible since mobile devices have become ubiquitous, it will allow Australians to extract value from a valuable asset that it should be recognised is owned by Australians, not by the entities that collect the data, and it will promote efficiency, innovation and competition in the adtech services sector (and other sectors including Australia's media sector), benefiting the Australian economy as a whole.***

6. The application of the CDR to location data, as Oracle has suggested in this submission, is an important step in moving forward to address the competition issues that exist in the Australian adtech services sector. However, it is not the only step that needs to be taken. The Australian Competition & Consumer Commission (**ACCC**) is currently undertaking an inquiry into the markets for the supply of digital advertising technology services and digital advertising agency services (**Adtech Inquiry**). Although the Adtech Inquiry is important in ensuring ongoing regulatory attention on the competition issues in the adtech sector, the ACCC should quickly move forward using its existing enforcement powers to address the

market failures that are already apparent in that sector. Regulators globally have recognised the need to take action, and are moving forward quickly.[1]

7. To effectively apply the CDR to location data, certain amendments are required to the Competition & Consumer Act 2010 (Cth) (**CCA**) and to the Privacy Act 1988 (Cth) (**Privacy Act**). These changes will provide important protections to Australians, including to limit the circumstances in which this category of personal information may be collected and used without the consent of the individual to whom the data relates.

8. We have explained in this submission the proposals that are being considered in the UK for the expansion of its Open Banking regime to information that is collected by digital platforms from consumers. There is an opportunity to work with the UK to ensure that both jurisdictions adopt a similar approach, reflecting the recommendations set out in this submission, which will be for the benefit of both jurisdictions, and ensure that compliance is easier to achieve for regulated entities. A common approach should act as an incentive for other jurisdictions to adopt similar regimes. However, Australia should not delay in moving forward in expanding the CDR, if the UK adopts a slower pace.

[1] For example, action is being taken at a Federal and State level in the United States: https://www.wsj.com/articles/justice-department-state-attorneys-general-likely-to-bring-antitrust-lawsuits-against-google-11589573622

Benefits arising from the application of the CDR to location data

Summary

As stated in the Explanatory Memorandum for the CDR legislation:

> ***the CDR aims to increase competition, enable consumers to fairly harvest the value of their data, and enhance consumer welfare.***[2]

For the reasons explained in this submission, implementing the CDR in relation to location data will achieve all of these aims:

- **consumer welfare will be enhanced as consumers will *for the first time* be given control of their location data, which is a very sensitive category of their personal information**
- **consumers will *for the first time* be able to fairly harvest the value of their location data**
- **if implemented together with other regulatory action which Oracle has called for in its submission to the ACCC's current Adtech Inquiry, innovation will be promoted and competition will be increased in the adtech services sector, leading to improved outcomes for the Australian economy and consumers**
- **there will be direct benefits across the economy from increased competition and innovation in the adtech services sector, including (but not limited to) in Australia's media sector**
- **data-driven innovation will be enabled in other sectors, through other uses of location data expressly permitted by Australian consumers.**

To ensure appropriate protections are in place for consumers, changes are required to Australia's competition and privacy regulation in conjunction with this expansion of the CDR.

What location data is collected?

General comments

9. A great deal of digital personal information is collected about Australians through their online interactions, including through their use of personal computers, mobile smart devices (and apps on those devices) and the myriad of Internet of Things (IoT) devices that Australians increasingly have in their homes, such as smart TVs. Much of this data is highly personal location data, identifying individuals and the details of their lives.

10. For example, Google is able to collect intensely personal renderings of an individual's online and offline life through the digital services that it offers. The information it collects, some of which is location data, includes:

    (a) data from every active user input into a Google service (in the form of, for example, watch history on YouTube or directions requests on Google Maps);

[2] Paragraph 1.3 of the Explanatory Memorandum for the Treasury Laws Amendment (Consumer Data Right) Act 2019.

(b) details regarding virtually every internet-connected user's private browsing activities on the desktop and mobile internet (whether through browsers or apps, including Google and third-party apps on Android and on other mobile operating systems (**OS**)); and

(c) for those Australian consumers with an Android mobile device, precise details about everywhere that individual has been, how they got there, and what they were doing there, which is obtained through the constant stream of granular location and activity data that Google gathers through such mobile devices (whatever privacy settings a consumer adopts).

11. The ACCC's Final Report from the Digital Platforms Inquiry includes an extensive list of data that Google collects about Australians.[3] All of this information is combined by Google across services, across devices, and over time, such that Google has a deep historical and highly specific picture of nearly every internet-connected individual's behaviour and interests. As Google's then-CEO said in 2010, "*We know where you are. We know where you've been. We can more or less know what you're thinking about.*"[4]

12. At the present time, Google primarily uses this personal information (including location data) for advertising purposes. The value of that information can be seen from Google's revenues. In 2019, the revenues of Alphabet Inc. (Google's parent company) were US$162 billion, almost all of which was generated from digital advertising.

Location data is valuable

13. Location data is one of the most valuable types of digital personal information that is collected by Google (and others).

14. As stated by the ACCC in its Final Report from the Digital Platforms Inquiry:

> *The increase in personal mobile devices such as smartphones, and the improvement in location tracking technology, has led to an increase in the location data collected and used. The prevalence of location data was flagged by Google CEO Sundar Pichai in his testimony to the United States Congress in 2018, where he stated that location is 'in the fabric of how people use the internet today'. Likewise the value of location data is indicated by the fact that sales of location targeted advertising reached an estimated US$21 billion in 2018.*[5]

15. Over time, location data creates a detailed profile about a consumer; where she lives, works, shops, eats, who she socialises with, and many other revealing insights about her pattern of life. The collection of location data over a period of time allows any third party who has access to that location data to infer sensitive and unique information about an individual.

16. For example, figure 1 below shows a small amount of data collected by Google, via an Android device, that initially seems benign (a record listing the Wi-Fi base station that Android device is connected to, along with a timestamp). Yet, if an individual connects to the same Wi-Fi access point at 9:00am Monday to Friday, it is clear the Wi-Fi base station likely represents the individual's place of work. Similarly, if an individual connects to the same Wi-Fi base station every day at 7:00pm and stays connected through the evening, the Wi-Fi base station is likely located in the individual's home.

[3] See Table 7.2 on page 380 of the Final Report from the ACCC's Digital Platforms Inquiry.

[4] Eric Schmidt, *Google CEO: "We Know Where You Are. We Know Where You've Been. We Can More or Less Know What You're Thinking About,"* BUSINESS INSIDER (Oct. 4, 2010), https://read.bi/2unSd5l.

[5] Final Report at page 385.

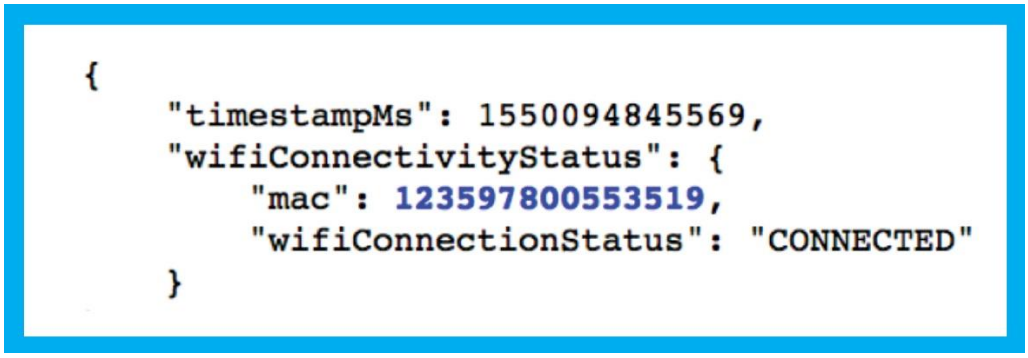

Figure 1: Test Android Device reporting Wi-Fi connection to Google

17. The following table shows in detail the location data that is collected from Android devices by Google.

Location Data Element	Collected by Google?
GPS Coordinates + Accuracy	YES
Altitude	YES
Wi-Fi Scans	YES
• **MAC Address**	YES
• **Signal Strength + Frequency**	YES
Bluetooth Beacon Scans	YES
• **MAC Address**	YES
• **Signal Strength + Frequency**	YES
Cell Tower Readings	YES
Barometric Pressure Readings	YES
Activity Readings + Confidence Level	YES
Source of Location Reading (Cell or Wi-Fi)	YES
Connection to Wi-Fi Access Points	YES
IP Address	YES
PlaceIDs	YES
Rate + Change in Rate of Collection	YES

Table 1: Types of location data collected by Google

18. Google is able to collect these types of location data from every Australian who has an Android device, as well as from Australians who use many of Google's other ubiquitous services, such as Google Maps.

19. As noted in the ACCC's Final Report from the Digital Platforms Inquiry, OECD research from 2013 found that 29% of the top rated paid apps and 60% of free apps in the Google Play Store sought permission to collect a user's location (and presumably therefore did collect it, even if it was not required for the delivery of the services offered by the app).[6] Google facilitates the collection of location data by app providers. If an app uses Google Android APIs to collect location data, Google receives a copy of this location data. As a result, Google has the largest pool of location data collected from consumers, and app providers have a subset that is non-

[6] Final Report at page 385.

unique. This means that although Google is not the only digital services provider that collects location data, Google has the ability to monetise consumer location data in ways others cannot (since they do not have a unique pool of location data that exceeds Google's).

Designation of location data

20. Under Part IVD of the CCA, location data derived from mobile devices, either collected via the OS itself or collected via apps meeting specific criteria, could be designated in accordance with section 56AC(2) of the CCA as a class of information. In the next few paragraphs, we explain how location data, and the class of data holders, could be described in a designation.

21. The location data covered by the designation made under Part IVD of the CCA will need to be very clearly defined in detail and should include at a minimum the different types of location data that is able to be collected by an OS provider, such as the information specified in Table 1 of this submission.

22. Google (and other service providers) may collect more location data than is strictly required to provide a particular service. For example, Google Maps is able to provide a more accurate and convenient service if it is able to use the location data of an individual while that individual is using Google Maps. However, Google may continue to collect location data from an individual even when that individual is not using Google Maps, that is, in circumstances where the app has no need to collect or store that location data. To avoid regulated entities raising arguments that only the location data collected from individuals which is directly used to provide a consumer facing service should be subject to CDR, the definition must clearly include *all* of the location data collected by a regulated data holder, irrespective of why that data was collected.

23. The designated class of information should not include any information that is *inferred* from location data. As mentioned previously, a great deal of information may be inferred about an individual by tracking their location – where they work, live and many other habits and interests. Applying CDR to such inferred data may stifle future developments whether in artificial intelligence (**AI**) or other areas which seek to transform location data into powerful inferences which can benefit society economically or socially.

24. Although, under Part IVD of the CCA, the class of consumers that may potentially be able to request the transfer of location data is large (including both individuals and entities), it is recommended that in this case the class is restricted to individuals only, given that location data is most relevant to individuals.

25. Location data is collected via smart devices on a continuous, real time basis. Although value is obtained from collecting that data over a long period (including to make inferences, as indicated above), it is particularly valuable when used on a real time basis – for example, to target advertising when a consumer is near a particular retail outlet or to provide information on traffic conditions as consumers travel in vehicles. As this is the case, the designated information should be *real time* location data.

26. The framework established by Part IVD of the CCA requires that businesses in a sector to which CDR applies must not only make consumer data available, as we have discussed in this submission, but must also make information on designated products publicly available. This is intended to facilitate comparisons being made between similar products offered by different providers, allowing informed choices by consumers. There is a diverse range of consumer facing products that are provided by the entities that collect location data (and other types of digital data). The rationale for the application of CDR to location data is not to facilitate comparisons between these existing consumer facing products, but to promote innovation and the provision of new products, as well as competition in associated markets such as in the

adtech sector. Therefore, in the application of CDR to location data, it would not be necessary to specify in the designation instrument particular products.

27. The designation instrument could provide that, initially, the persons that currently hold the designated information (the data holders) would be OS providers, that is, primarily Google (in relation to the Android OS) and Apple (for iOS). Providers of any app that collects location data and associates it with an individual or an account of an individual (i.e., where the data is not collected solely on an anonymised basis) that meet a particular threshold limit could be included on a delayed basis. For example, at a later time, data holders could be extended to include operators of apps with 500,000 or more Australian subscribers (or another appropriate number that does not place undue burden on small businesses or start ups). This would be a similar approach to that adopted for the application of the CDR in open banking, where a phased approach is being adopted, with the 4 major domestic Australian banks being subject to the regime at any earlier point than smaller banks.

28. As a second stage, the CDR could at a future point in time potentially be applied to a broader category of digital personal information that is collected from Australian consumers through their use of digital services, provided that broader category was carefully scoped and clearly defined.

The importance of location data for targeted advertising

Location data collected by service providers such as Google is of great value in delivering targeted online advertising.

29. Taking Google as an example, it is easy to demonstrate the importance of location data for targeted online advertising. Google's ability to collect location data allows Google to claim in its marketing materials to advertisers that it can determine with a "*99% certainty*" whether a consumer to whom an ad has been displayed subsequently visits a brick-and-mortar store.[7] Google's store visits conversions are based on matching consumers' Android or iOS location history with "*the exact dimensions of over 200 million stores globally.*"[8]

30. So, for example, after displaying an ad for Nike football shoes, Google is able to verify the effectiveness of the ad by confirming that a consumer checked out the shoes online on his or her mobile device, then walked to a specific shopping mall, that he or she went to the fifth floor of that shopping mall and that he or she visited the Nike store located on that fifth floor. This information allows the advertiser – in this case Nike – to determine whether its ad campaign was successful. As Google itself says, its adtech services allow marketers to "*close the loop between online ads and offline sales.*"[9]

31. Location data, of itself, is also important to advertisers for another reason. Location data enables advertisers to target ads to users in a specific location irrespective of any other characteristics of those users. For example, advertising may be targeted to consumers in a particular country, region, radius around a specific location or near specific business addresses, irrespective of the other characteristics of the individuals.[10] Therefore location

[7] https://www.blog.google/products/ads/new-digital-innovations-to-close-the-loop-for-advertisers
[8] https://www.blog.google/products/ads/new-digital-innovations-to-close-the-loop-for-advertisers
[9] https://adwords.googleblog.com/2016/09/New-Digital-Innovations-to-Close-the-Loop-for-Advertisers.html.
[10] See for example as advertised by Google: https://ads.google.com/intl/en_us/home/how-it-works/: Here it states: "For your ad to perform well, it has to find the right audience. Google Ads lets you choose the location where your ad will appear, including within a certain radius of your store or covering entire regions and countries."

data is very valuable, even where it cannot be combined with other types of personal information in relation to an individual consumer.

32. The importance of location data is also demonstrated by statements Google makes to advertisers regarding this type of data. For example, Google states in the information that it provides to advertisers:

> ***About targeting geographic locations***
>
> *Target your ads to people in—or who've shown interest in—geographic locations relevant to where you do business. You can select whether you'd like your ad to appear for someone's physical location, locations of interest, or both. Location targeting can help you make sure your ads are relevant to the people who see them—which can help boost your campaign's value.*[11]

33. The importance of all types of digital personal information, not only location data, has recently been recognised by both the Government and the ACCC in the context of the proposed mandatory code of conduct to address bargaining power imbalances between digital platforms and media companies.[12] One of the issues that the mandatory code will address is the provision to media companies of information which the digital platforms have collected in connection with consumers accessing the content of the relevant media company. Media companies and the platforms have not been able to reach agreement on this issue (amongst others), indicating that this information has a significant value in the context of targeted advertising.

The benefits of providing consumers with greater control over their location data and the ability to fairly harvest the value of their location data

Consumers may provide their location data to Google at less than the fair value of that location data because of market failure. The CDR may assist in addressing this market failure.

Market failure: lack of information and bargaining imbalance

34. It is of course true that digital platforms and other service providers that collect location data provide a wide range of digital services to consumers at zero monetary cost in exchange for those consumers providing their location data.

35. Numerous questions arise in this context. First, do consumers actually understand that this is the deal they have made with such service providers and do they truly understand how much information service providers such as Google collect? Are the "free" digital services really adequate compensation for the data that consumers provide? Is the consent a consumer provides to the collection of their location data truly "free" consent?

36. In the Final Report from the Digital Platforms Inquiry, the ACCC concluded that there may exist a market failure. In the ACCC's view, consumers, in agreeing to provide their location data to digital platforms in return for the provision of services, may not be making informed choices. There is a bargaining power imbalance between the platforms and consumers (i.e., so consumers feel they have no choice but to agree to the data collection), there is a significant

[11] https://support.google.com/google-ads/answer/2453995?hl=en

[12] https://ministers.treasury.gov.au/ministers/josh-frydenberg-2018/media-releases/accc-mandatory-code-conduct-govern-commercial

information asymmetry between the platforms and consumers and consumers also have difficulties in assessing the value of their data once it is in the hands of the platforms.

37. Not only do consumers have difficulty in assessing the costs of providing their information (both in the case of digital platforms and to other providers of digital services) but they have difficulty in assessing the *value* of that information. As a consequence, the ACCC concluded consumers will be better off when they are sufficiently informed and have sufficient control over their user data, so that they actually can make informed choices that align with their privacy and data collection preferences. Applying the CDR to location data, and potentially to other carefully defined categories of digital personal information at a later stage will assist in addressing this market failure.

Significant benefits from initially applying the CDR to location data

38. As is made clear in the Final Report from the ACCC's Digital Platforms Inquiry, one of the most concerning types of data collection from the perspective of Australian consumers is the collection of location data. The ACCC's consumer survey indicated that an overwhelming percentage of Australians who use digital platforms considered the monitoring of offline location and movement without the user's consent to be a misuse of their data.[13] Implementing the CDR to location data has additional benefits for consumers as it will mean that a key area of concern for most consumers in relation to the collection of digital personal information is addressed quickly.

39. Google has been tracking the physical location of consumers for approximately 15 years, since it first started tracking IP addresses.[14] Notwithstanding the concerns of Australian consumers, at the current time, location data continues to be collected by Google in accordance with its privacy policy, with Australians having only a limited ability to control that location data collection and, in a practical sense, no control over how that location data is used once it is collected. The privacy policies of many apps also allow for broad rights to collect location data (even if such location data is not required for the efficient use of the relevant app).

40. Location data has significant value. Therefore applying the CDR to location data is likely to provide the most immediate benefits to consumers to be able to fairly harvest the value of their digital personal information. Other businesses may be willing to provide consideration that particular consumers value highly, for example, the exchange of location data for a free or subsidised data plan may be one example of what others would be willing to offer consumers for their location data.

Inability to address identified issues through changes to the Privacy Act

41. The ACCC expressed the view in the Final Report from the Digital Platforms Inquiry that Australia's existing regulatory framework for the collection, use and disclosure of user data and personal information, that is, the Privacy Act 1988 (Cth) (**Privacy Act**), does not effectively deter certain data practices that exploit the information asymmetries and bargaining power imbalances between digital platforms and consumers. We agree this is correct and, even when the amendments that the Government has announced it proposes to make to the Privacy Act are implemented, the issues the ACCC has identified will not be fully addressed. This is because the Privacy Act provides only limited rights to Australians; it does not for example allow directions to be given by consumers to those business that collect their location data and other digital personal information and does not address the bargaining power imbalances between consumers and those businesses. Applying the CDR to location data, and in future potentially other types of digital personal information, provides the opportunity to address all of the issues that were identified by the ACCC. To enable this to

[13] 86% of this category of Australians hold this view, see page 385 of the Final Report.
[14] Final Report, see Table 7.2 on page 380.

occur, the regulatory changes that we have discussed in this submission will also need to be addressed.

Designation of location data would be privacy enhancing

42. Designating location data, and potentially other digital personal information in future, will enhance the privacy protections that Australians have.

43. If location data is designated, it will only be able to be transferred in the manner permitted by the CDR framework. In addition, location data may only be transferred to accredited persons, who must hold the data (and data derived by the relevant accredited person from it) in accordance with the privacy safeguards in Part IVD of the CCA and any additional privacy requirements of the consumer data rules made by the ACCC. The imposition of such additional privacy requirements, together with the monitoring that the ACCC is empowered to carry out, will assist in ensuring that the accredited entities can be trusted to protect the location data that is provided under the CDR.

44. Due to the time-sensitive nature of location data, it likely will be necessary to address the timeliness of the data transfers requested by consumers in the ACCC's consumer data rules. Those rules should operate to prevent a situation where location data transferred by Google (or any other data holder) to an accredited entity was delayed in a manner that gave a competitive advantage to Google due to its control over and proximity to the valuable data stream.

45. A Data Standards Body assists the Data Standards Chair in making data standards for the CDR. The data standards prescribe the format and process by which CDR data is to be shared with consumers and accredited data recipients within the CDR system and therefore is able to be designed to ensure that security and privacy are protected.

46. Clearly, these requirements will significantly enhance the privacy protections for Australians, as compared to the current situation. At the current time:

    (a) Location data may be transferred by any person that collects it, provided that where the person collecting the location data is bound by the Privacy Act, its privacy policy permits this. There is no requirement that the transfer occurs in a particular way and therefore no requirement that the protections the Data Standards Body and Chair would require for the transfer of CDR data are applied.

    (b) There is currently no requirement under Australian law that any third party recipient has any accreditation of any sort.

    (c) A consumer has no say in how a third party recipient may deal with the data, provided that (if the recipient is in fact subject to the Privacy Act) such use complies with that third party's privacy policy, over which the Australian consumer has no control.

Summary of benefits

47. From the perspective of a consumer, applying the CDR to location data has the beneficial outcomes set out below, which are able to be achieved within a framework that will enhance consumer privacy protections:

    (a) Providing for the CDR to apply to location data will improve transparency and limit the information asymmetry between OS providers, digital platforms (and other relevant service providers) and consumers, as these providers will be required to disclose to consumers exactly the location data that is collected, to allow each consumer to make a decision as to whether she requires that location data to be transferred to the consumer herself or to other parties. Consumers will in this way also know who receives their highly sensitive location data.

(b) Giving consumers the right to require their location data to be shared under the CDR will go some way towards addressing the power imbalance between digital platforms (and other relevant service providers), particularly dominant service providers such as Google, and consumers. As we have suggested in this submission, to properly address this issue regulatory change should be implemented to allow consumers to elect for location data to be *transferred*, rather than shared. That is, a consumer should be able to require that a data holder does not retain the location data that is transferred to a third party (or to the consumer herself). Only in that way would a consumer truly be in control of her location data.

(c) This will also enable the question of the value of location data to be determined. Google and other digital service providers argue that the services they provide in exchange for location data (and the collection of many other types of digital personal information) they collect from consumers is fair consideration for that data. It is simply impossible to determine whether or not that is true because there is no competitively efficient market for any form of digital personal information that Google and other service providers collect, given the information asymmetries and imbalance in bargaining power discussed above. If consumers had the right to provide their location data to third parties, then a competitively efficient market would come into existence and consumers would be able to better assess the value of that information and fairly harvest the value of that information.

Additional competition, including innovation, benefits of applying the CDR to location data

48. Applying the CDR to location data will improve efficiency in relevant markets and foster both competition and innovation. This inevitably will assist consumers and the economy as a whole.

49. The market for the "sale" of the location data of Australian consumers is not efficient for the reasons outlined earlier in this submission. As consumers do not receive clear information on when their location data is collected or who is collecting or receiving it, do not have visibility on how that location data is used (including by third parties to whom the location data may be transferred after it is initially collected), have little choice as to whether to agree to provide their information if they wish to use a particular digital service and, in reality, cannot require any person that collects that location data to provide it the consumer[15], then that market is not efficient. Making this market more transparent and increasing the bargaining power of consumers, by providing a greater degree of control to consumers over who may receive their location data, and requiring third parties to compete for the right to receive it, will improve efficiency.

50. Applying the CDR to location data will also assist in facilitating the conditions for competition, and therefore have an efficiency dividend, in the adtech services sector. As mentioned previously, the location data that is collected from consumers is important in the delivery of adtech services. At the current time, neither Google, nor other digital service providers, voluntarily transfers any of this information and consumers cannot require them to do this.

51. In its Final Report from the Digital Platforms Inquiry the ACCC made the important point that data portability may have the effect of helping rival firms to Google in the adtech market overcome the competitive disadvantage that they have because of Google's overwhelming

[15] As explained in Oracle's submissions to the Digital Platforms Inquiry (including its submission to the Preliminary Report, see here: https://www.accc.gov.au/system/files/Oracle%20Corporation%20%28March%202019%29.PDF) Google provides access to *some* location and other data that Google collects from consumers but not *all of* that data.

volume of consumer data.[16] This is likely to make the adtech services market more competitive and more efficient, as prices should be reduced for adtech services that rely on location data. Alternative adtech services providers may also be able to provide greater value to publishers, including traditional media companies, which will of course provide benefits to those publishers. Those benefits will have the potential to assist in reversing, at least to some extent, the under-provision of news and journalism that has been highlighted in the Final Report, which will have broader societal benefits.

52. Adtech services providers, and others, are likely to also be able to use valuable location data for the development of innovative products and services for Australians. Of course, it is impossible to specify what all of those innovations may be in this submission. One example of where there would be benefit from increased access (strictly in accordance with the regime provided for in Part IVD of the CCA) is likely to be in the area of AI. AI relies on the provision of high quality data, such as would potentially be available if the CDR was applied to location data.

53. The other innovative uses of location data (and other digital personal information, if ultimately the CDR was to be applied to such other data) will only become apparent when this data is actually available – but, again, there is significant potential for this to be the catalyst for innovation and therefore economic growth. In the current COVID-19 pandemic for example, there would be clear benefit if consumers actually already had the right to direct real-time streams and require the transfer of, at least, their historical location data. If this could be required, the Government's job of infection tracking would be made considerably easier.

54. Arguments may be raised that applying the CDR to location data may chill competition, as competitors in the adtech services market and other digital markets will cease to provide competitive products that would allow them to directly collect location data from consumers as they will instead rely on the potential to obtain this information under the CDR. However, such an argument should not be accepted. Demand for location data is high because it is so valuable in the adtech services market (and in future may have a value in other markets too). Google's ability to collect location data arises from its dominance in certain markets, including the market for licensable OS on mobile devices, where it has ownership of Android OS, and in consumer facing markets, such as Google Maps. In the short to medium term it cannot be expected that other service providers would be able to compete to provide alternative services in each of these areas where Google is dominant – for example, to develop an alternative licensable mobile operating system that was widely adopted would take a significant amount of both time and capital. However, given the value of location data, there is no doubt that there are many companies that would actively compete, via the provision of innovative products and services, for consumers to agree to provide that information to them.

55. Although applying the CDR to location data will be a very important step in promoting competition in the Australian economy, this will not be a complete answer to the competition problems that currently exist in the Australian adtech services market and, indeed, exist globally in that market. Oracle's submission to the ACCC's Adtech Inquiry addresses the broader regulatory action that the ACCC should take – that action should be taken in addition to applying the CDR to location data and potentially other types of digital personal information in future.

[16] Final Report, see page 115.

Necessary regulatory change

56. To maximise the effectiveness of the implementation of the CDR to location data (and potentially other types of digital personal information in future) it is necessary to make a number of regulatory changes, which are outlined in this section of Oracle's submission.

Changes to Part IVD of the Competition and Consumer Act

Transfer, not sharing, of location data

57. Consumers should have the right to require Google and other digital service providers that are subject to the CDR to transfer the location data of the relevant consumer, rather than simply share that data. This is, in a practical sense, a specific application of the recommendation made by the ACCC in the Final Report from the Digital Platforms Inquiry that individuals have the right to require erasure of the personal information held about them. That is, an individual would be provided with the option to require the original data holder to erase information that is either transferred directly to the individual or transferred to a third party under CDR.

58. The ACCC recommended a right of erasure on the basis that it would provide consumers greater control over their personal information and that it would be likely to help mitigate the bargaining imbalance between consumers and digital platforms.[17]

59. Although the Government, in its response to the Digital Platforms Inquiry, stated that the right to erasure would be considered as part of the proposed longer term reform of the Privacy Act, the Government qualified this on the basis that consideration would need to be given to potential freedom of speech concerns, challenges to law enforcement and national security investigations where personal information was erased before an investigation was completed and the practical difficulties that could arise from imposing this obligation.

60. None of the reservations that the Government expressed in relation to a broad right of erasure would apply in relation to the specific application of the right of erasure in this case, given that location data is not of a type of information that would raise freedom of speech concerns, the data would not be deleted entirely (as the transferee would still have it) and there would be unlikely to be difficulties in imposing a deletion requirement on the transferred information, which would need to be specifically identified to be transferred and therefore could easily be erased.

Geographical limitations

61. Geographical limitations are imposed on information that may be designated under section 56AC(2) of the CCA. In so far as is relevant here, information will only be included in a designated class if it:

    (a) has at any time been generated or collected wholly or partly in Australia (or the external Territories) and relates to one or more Australian persons (other than the persons who so generated or collected it); or

    (b) has only ever been generated and collected outside Australia and the external Territories and has been so generated or collected by or on behalf of one or more Australian persons *and* either relates to one or more Australian persons (other than the persons who so generated or collected it) or relates to goods or services supplied, or offered for supply, to one or more Australian persons.

    (c) "Australian person" is defined in section 56AO(5) of the CCA to include a body corporate established under an Australian law, an Australian citizen or permanent

[17] See page 471 of the Final Report.

resident, or a person who is ordinarily resident within Australia (or an external Territory) or a Government entity.

62. The application of these geographical limitations would appear to mean that location data collected from the devices of Australian persons outside Australia (and the external Territories) by a person who is not an Australian person would not be designated information.

63. This type of geographical limitation makes little sense in relation to location data. In fact it would be likely to make it more difficult, rather than less, for those entities falling within the data holder category to determine what data would need to be transferred if this geographical limitation was retained as, where the data holder is not an Australian person, it would need to distinguish between data collected from an Australian person when that person was in Australia and data collected when that person was not in Australia, which is a distinction such entities would generally be unlikely to make. Therefore, for the purposes of the application of the CDR to location data, the only requirement should be that the information is collected *from* an Australian person. Of course, in any event, if the CDR regime was also adopted in other jurisdictions, at least in its application to location data, then the question of geographical restriction would be less relevant.

Changes to the Privacy Act

"Personal information" under the Privacy Act

64. Recommendation 16(a) in the ACCC's Final Report was that the definition of "personal information" in the Privacy Act should be clarified to ensure that it captures technical data such as IP addresses, device identifiers, location data and other online identifiers that may be used to identify an individual. In the Government's response it was stated that consultation would occur on that proposal, provided that any amendments made do not impose an unreasonable regulatory burden on industry.

65. Oracle's view is that such data, including in particular location data, where it is able to be directly associated with an identified individual or an individual who is reasonably identifiable, will already fall within the definition of personal information. Nonetheless, if CDR is applied in the manner that we have outlined in this submission, it would be important to expressly include all location data as personal information under the Privacy Act to ensure that the Privacy Act, like the CDR legislation, recognises that location data should receive the highest levels of protection under Australian law.

Rights to object to collection and disclosure of personal information

66. Recommendation 16(c) in the ACCC's Final Report was that the Privacy Act should be amended to strengthen consent requirements and pro-consumer defaults, including to require that consent to personal information collection is "freely given", that is, that the provision of services or goods must not be conditional on consent being provided to the collection and processing of personal information that is not necessary for the provision of those services/goods. As in the case of recommendation 16(a), the Government response was that it supports this recommendation in principle. The Government qualified this by stating that this would be in the context of ensuring that the requirements did not impose a significant regulatory burden and did not add to individuals suffering from "consent fatigue".

67. An examination of this recommendation is particularly important in the context of the application of the CDR to location data. Location data, and other types of personal information is collected by digital services providers for two reasons. The first is for the purpose of using that information to provide a particular digital service that has been directly requested by the relevant consumer. The second is to use that data for other reasons related to the business of the digital service provider, particularly the delivery of targeted advertising.

68. To ensure that the CDR, when applied to location data, provides the intended benefits to individuals (and without limiting the rights of individuals to require that data is transferred rather than shared, as outlined previously), individuals should have the right to:

    (a) restrict the purpose for which location data is used to the purpose of providing the relevant service; and

    (b) object to location data being collected and then used or transferred to third parties for purposes other than providing the relevant service.

69. Tied to the above, an individual should have a legally enforceable right to be able to continue to use the relevant digital service in the event that she does not agree that location data could be used other than for the purpose of provision of that service. If this, more limited, alternative to recommendation 16(c) was adopted, this would address the concerns that were identified in the ACCC's Final Report whilst at the same time ensuring that an unreasonable regulatory burden is not imposed economy wide and limiting the likelihood of "consent fatigue". This requirement should be supported by a digital platform specific code, as discussed immediately below.

Privacy code for digital platforms

70. The ACCC recommended that an enforceable code of practice be developed specifically for digital platforms (Recommendation 18). Although other types of digital service providers collect location data and other types of personal information, digital platforms, particularly Google, collect more of this information from consumers than anyone else. Therefore it is appropriate that such a code applies only to digital platforms. A code would be important in the context of the application of the CDR to location data, particularly in relation to consent requirements and opt-out controls. The Government's response to this recommendation was to agree that legislation to provide for such a code would be introduced in 2020.

71. The code should be required to address the following:

    (a) The consent requirements of the code should reinforce that consumers must opt-in for any data collection and use, including location data collection and use, that is for a purpose other than the purpose of supplying the relevant consumer-facing services (with such services to exclude targeted advertising). The code should also state that digital platforms may not refuse to provide services where this opt-in consent is not provided.

    (b) Reinforcing subparagraph (a) above, as recommended by the ACCC, the code should require that digital platforms give consumers the ability to select global opt-outs or opt-ins, such as with regard to the sharing of personal information, including location data, with third parties for targeted advertising. Again, the code should make clear that digital platforms may not refuse to provide services where this opt-in consent is not provided.

Potential for international coordination

72. Although the application of the CDR in the manner that we have suggested in this submission will have significant benefits for Australians, and the Australian economy, there are also benefits in working with other jurisdictions to ensure that a consistent approach is adopted.

73. The UK's Competition & Markets Authority (**CMA**) in late 2019 released its Interim Report from its Online Platforms and Digital Advertising Market Study. Appendix L of that Interim Report considered two different proposals for improving personal data mobility, the first of which would be similar to the application of CDR to digital personal information, at least where such information is collected by digital platforms, in the manner outlined in this

submission. The view of the CMA was that adopting one or both of the proposals could help better protect privacy whilst increasing competition and ensuring that consumers are able to benefit to a greater extent from the value of their data. We agree this is achievable, but recommend that the UK approach more closely align with that of the CDR approach outlined in this submission.

74. There would be benefits in engagement with the CMA to enable both The Treasury and the CMA to consider whether it would be possible to develop a consistent regime. Ultimately, the adoption of a consistent regime across multiple jurisdictions will assist in reducing the costs of the digital service providers that are subject to the CDR. However that consultation should not delay the adoption of these important reforms in Australia.

Thank you very much for considering this submission. Oracle would be very pleased to discuss any aspects of the submission with The Treasury if requested.

Oracle Corporation

10 June 2020