Google Australia Pty Ltd
Level 5, 48 Pirrama Road
Pyrmont NSW 2009

Tel: 02 9374-4000
Fax: 02 9374-4001
www.google.com.au

Digital Platforms Inquiry
Submission on proposed privacy regulation

Introduction - Smart Regulation for Privacy

The ACCC's Preliminary Report proposes legislative and other data privacy amendments and recommendations focused primarily on digital platforms, which would not have universal application to all companies that collect personal data. Google strongly believes that privacy protection for consumers should apply universally and consistently to digital platforms and all other organisations that collect and use personal data, and that are currently subject to the Privacy Act.

As detailed in this paper, many organisations besides digital platforms collect personal data about individuals and use that data in similar ways to digital platforms; there is simply no good reason to subject the collection, processing, and use of personal data by those companies to different rules. The risks of harm from using personal data are not specific to digital platforms. Moreover, as a practical matter, it is inevitable that the introduction of privacy rules that apply only to certain digital platforms would extend beyond those digital platforms, requiring other businesses to incur costs and invest resources in ensuring compliance with new privacy standards applicable under those rules.

This paper also responds to suggestions by some third party stakeholders that the European Union's General Data Protection Regulation 2016/679 (**GDPR**) should be adopted in Australia. Google supports smart regulation and innovative ways to address consumer concerns related to privacy and data protection in Australia and around the world—to this degree, Google is of the view that any adoption of aspects of GDPR in Australia should be carefully considered. To the extent that the ACCC is concerned about privacy and user data in Australia, it should consider recommending that there be a separate review of privacy laws. In this separate review, there would be time and resources for a full and detailed analysis of proposed approaches, including potential adaptations to GDPR as appropriate (which will become more apparent and understood in time).

Privacy protection for consumers should apply to all companies that collect data

The ACCC's Preliminary Report proposes legislative and other data privacy amendments and recommendations focused primarily on digital platforms, which would not have universal application to all companies that collect personal data. With respect to personal data, and the importance of ensuring that same data, wherever held, is treated consistently and equally, any fundamental changes should be of universal application. Individuals should be able to expect the same rights over their personal data, regardless of what organisation is processing it.

Many varying organisations collect personal data about individuals, and often, those organisations collect the same types of personal data, regardless of their industry or sector. A table setting out details of some of the personal data collected by supermarkets, banks, airlines, and media companies, online and offline, is provided in **Annexure A**. The personal data these companies collect may be used in a wide variety of ways, which may include targeting or personalising advertisements, or offering goods or services. Because the data can be used in similar ways by different organisations, there is no good reason to subject the collection, processing, and use of personal data by these companies to different rules or codes of conduct.

If the ACCC's goal is to protect consumers and their data, then the same privacy rules should apply to that data wherever it is held. Applying different rules to the data held by one company, but not to the same data held by a different company, would be problematic. It would result in a significant regulatory gap and would fail to adequately protect consumers. It would also be anomalous and confusing for consumers, if the rules that applied to the collection, retention and use of their personal data were different depending on whether the organisation was a digital platform, as opposed to, for example, a supermarket, bank, airline, or media company.

Privacy rules that apply only to particular digital platforms would have downstream consequences for other companies

Imposing a new set of privacy rules that would apply only to particular digital platforms, such as Google, will have downstream consequences for other companies, particularly smaller companies and vendors that seek to do business with digital platforms.

To illustrate, we explain below how the introduction of a GDPR-like privacy law applicable only to Google and Facebook (and any other digital platforms that meet a set threshold) would impact Australian businesses not directly subject to such a law.

Under the GDPR, "controllers"[1] (including Google) are required to only use "processors"[2] (including any other businesses that Google works with, e.g., a vendor providing services) that can provide sufficient guarantees that the "personal data" will be processed in accordance with the GDPR.[3] In practice, this is largely achieved by controllers imposing contractual obligations on processors.

The GDPR also enables enforcement actions to be brought directly against processors (meaning that separately from Google, a business who is a processor for Google is directly responsible for compliance with certain provisions of the GDPR). Even if the organisation is not a processor for Google, but is a business partner, the organisation could still be considered a "joint controller" with Google. In that case, Google and the organisation would have to determine how to allocate their respective responsibilities in respect of compliance obligations under the GDPR. Regardless of how the compliance obligations are shared, both firms would be equally responsible to respond to individuals exercising their privacy rights under the legislation.

Even if the above-mentioned aspects of the GDPR were not implemented in Australia (with a view to minimising impact on other businesses), Google and other digital platforms subject to the new rules would need to, in order to ensure compliance with the rules, secure contractual assurances from their business partners that they will manage data in accordance with the rules. The practical effect would be that any party seeking to partner with Google (and other digital platforms subject to the new privacy rules), on any activities involving personal data, would need to incur cost and invest resources in establishing a compliance program that satisfies the standards under the new rules.

Additionally, it is impractical for firms to have two different tiers of privacy compliance programs. Consequently, firms would need to make a choice between not partnering with Google (and other digital platforms subject to the new rules), or partnering with Google (and other digital platforms subject to the new rules) and establishing an adequate compliance program—which would also likely mean that other smaller businesses they work with will also be affected (e.g., Firm A provides services to Google and, accordingly, has to comply with the new rules. When Firm A subcontracts work to Firm B, Firm B would also need to comply with the new rules).

---

[1] Under the GDPR, "controller" is defined as a person who jointly with others determines the purposes and means of the processing of personal data, which person may be designated by EU or Member State law.

[2] Under the GDPR, "processor" means a person who processes personal data on behalf of the controller, and "processing" means any operation or set of operations performed upon personal data (which explicitly includes references to the storage or structuring of data).

[3] See Article 28 of the GDPR ("*Where processing is to be carried out on behalf of a controller, the controller shall only use processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject*...").

Accordingly, it is inevitable that the introduction of privacy rules that apply only to certain digital platforms would, as a practical matter, extend beyond those digital platforms, requiring other businesses to incur costs and invest resources in ensuring compliance with new privacy standards applicable under those rules. This reinforces the impetus for having privacy rules apply universally and consistently to all organisations that collect and use personal data, rather than only to a subset of them.

Google's perspectives on the GDPR

At the Privacy Roundtable, and in third-party submissions to the ACCC, some stakeholders and the ACCC expressed interest in the GDPR as a style of privacy protection for which Australia could aim.

Google is committed to complying with the GDPR,[4] and strives to do so in respect of its global operations, with a few exceptions limited to Europe. Google takes the same approach to consent in account creation, account controls, data minimisation, data deletion, and other requirements under the GDPR across its global operations.

In particular, Google considers that the following aspects of the GDPR strike the right balance between the interests of consumers ("data subjects") and organisations that collect, process, and use personal data ("controllers" and "processors"), and merit consideration:

1. The multiple legal bases for data processing, including, in particular, "legitimate interests", rather than requiring consent for all uses of personal data.

    a. There is growing recognition among regulators, researchers, and organisations that asking individuals to opt-in for all uses of information is impractical and leads to fatigue that diverts attention from the most important user choices. For example, some data processing is necessary to make products work and to ensure that they are secure and reliable. Users can generally accept and even expect and consider it reasonable that some personal information needs to be processed by a company providing a product or service. In this scenario, asking users to provide consent presents the odd decision of "agree" or "don't use the service." This could have the perverse effect of teaching users to simply click "agree" to everything without paying attention.

    b. The GDPR requires businesses and organisations to incorporate transparency and fairness into their practices, and permits processing that balances the "legitimate interests" of the organisation processing the data against the impact of that processing on the rights and interests of the individual. Where processing of personal data satisfies this balancing test and respects privacy principles, the

[4] See: https://privacy.google.com/businesses/compliance/#!?modal_active=none

business or organisation may rely on legitimate interest as the legal basis for the processing, which would be an alternative to consent. Google is supportive of privacy laws encouraging businesses and organisations to balance these same interests.

2. The GDPR prescribes different levels of controls rather than a one-size-fits-all approach, taking into account the type of data being processed and the risk of harm.

    a. For example, more restrictive rules apply to the processing of "sensitive data."[5]

    b. The GDPR's mandatory data breach notification rules[6] are also calibrated based on the risk of harm to individuals.

3. The GDPR carefully considers exemptions and exceptions for rights like access to data and deletion of data that allow for necessary business processing.

    a. For example, where a data subject withdraws consent on which the processing is based, the data controller need not necessarily delete the data if there are other legal bases for processing. See Article 17[7] for the full list of other exemptions and exceptions.

Google would not recommend the wholesale adoption of the GDPR in Australia. There are meaningful cultural, economic, and political considerations that must be factored into the process of adopting any important legal regime—and the GDPR is tailored to the economy and concerns of EU citizens, not a global audience. To the extent it is concerned about privacy and user data in Australia, the ACCC could consider a separate review of privacy laws. In this separate review, there would be time and resources for a full and detailed analysis, as well as a wide public consultation, of proposed approaches, including potential adaptations to GDPR, as appropriate.

Importantly, the GDPR was not designed to be a global standard for privacy protection. Implementing the GDPR does not mean achieving interoperability. In fact, the GDPR establishes barriers to cross-border data flows that complicate the conduct of business across countries. In the Asia-Pacific region, very few countries have been deemed GDPR-adequate or expressed intentions to become GDPR-adequate in the near future. Countries that have been deemed adequate also do not have laws that are identical to the GDPR. It is also important to remember that the GDPR is a data protection law, not a consumer protection law. Many of the issues addressed by the GDPR are less relevant to the experience of users, and more about the management of data (for example, restrictions on international data transfers). Implementing a GDPR-like law in Australia before other countries in the Asia-Pacific region

[5] See Article 9 of the GDPR.
[6] Article 33 of the GDPR.
[7] https://gdpr-info.eu/art-17-gdpr/

would create complexity and interoperability issues for any company with operations in the region, resulting in inefficiencies and increased compliance costs, rather than addressing these issues.

Finally, while the GDPR has been widely discussed for years and feels like a familiar topic, it is a relatively new law in effect for less than one year. The GDPR only came into effect on 25 May 2018, and there remains a lot of uncertainty about the interpretation of key obligations and the practical effects on businesses and markets. At the very least, these areas of uncertainty, and the practical challenges apparent to date, ought to be factored into any consideration of GDPR as a benchmark or starting position when evaluating whether (and if so, what) changes should be made to Australia's privacy laws. Thus, it may be premature to recommend its wholesale adoption in Australia.

As stated in Google's submission in response to the ACCC's Preliminary Report, Google supports smart regulation and innovative ways to address consumer concerns related to privacy and data protection in Australia and around the world. This includes the development of baseline "rules of the road" for data protection, like those that currently exist in the *Privacy Act 1988* (Cth). Google's "Framework for Responsible Data Protection Regulation" (**Framework**), and accompanying blog post published in September 2018,[8] outline Google's views on privacy reform. The Framework addresses the requirements, scope, and enforcement expectations that Google believes should be reflected in all effective data protection laws. It is also based on Google's experience providing services that rely on personal data and its work to comply with evolving data protection laws around the world, including the GDPR. Google considers that its Framework incorporates the best of the GDPR and other international regimes, and Google would encourage consideration of the Framework in assessing proposed amendments to Australia's privacy laws.

10 May 2019

[8] See: https://www.blog.google/outreach-initiatives/public-policy/proposing-framework-data-protection-legislation/

Annexure A
Examples of personal information collected by other organisations

This table sets out details of some of the personal data collected by other organisations, including supermarkets, banks, airlines, and media companies, online and offline. The personal data these companies collect may be used in a very wide variety of ways, which may include, targeting or personalising advertisements or offering goods or services. Because the data can be used in similar ways across industries, there is no good reason for subjecting the collection, processing, and use of personal data by these companies to different rules or codes of conduct from those that apply to digital platforms.

Organisation	Type of personal information collected (as per company's privacy policy)	What information is used for (as per company's privacy policy)
Airline	● General information about the user (name, title, gender, date of birth, contact details, passport or other ID details) ● Contact details (phone number, address, email address and social media handle) ● Travel details (travel itinerary, baggage, seat preferences, seat and meal requests) ● Health and dietary information (dietary requirements and health information) ● Payment details (credit or debit card number, expiry date) ● Use of products and services (e.g., inflight entertainment systems, CCTV images in airport lounges and on-board, previous travel arrangements) ● Interactions with Airline (feedback, complaints, compliments, claims, responses to market surveys, records of correspondence etc ● Interests (destinations visited and products bought) ● Website and mobile apps (geo-location, IP address, mobile number or ID, details of how it is used, any access to third party sites from there) ● Programs and clubs (membership number and participation) ● Employment information (about relationship with corporate or government clients, professional title and work contact information) ● Incidents (involved in or witnessed) ● Wifi use (information about "you," the device and how wifi service is used)	● To provide and administer travel products and services ● For marketing purposes (updates and offers, competitions, promotions, events, newsletters and other communications) ● To provide customer support ● To comply with legal obligations and safety and security purposes ● To operate and facilitate participation in programs and clubs (i.e. to track benefit accrual and redemption activities) ● To conduct market, consumer and other research (to improve products etc) ● To ensure website content is relevant ● To manage any shareholding in Airline

Organisation	Type of personal information collected (as per company's privacy policy)	What information is used for (as per company's privacy policy)
	● Shareholders (obtained through share broker to register and verify interest in Airline securities; name, address, number of shares held, tax file number and bank account details) ● Sensitive personal information (eg where medical or access assistance is requested; dietary requirements for religious reasons)	
Airline Frequent Flyer Program	● Personal information to generate insights about the Member to understand their preferences and interests, to assess applications, to award points, etc. ● When the Member is logged into their Airline Frequent Flyer account ● Information from third parties, Airline's related bodies corporate and Jetstar branded entities, partner airlines, third parties providing services for Airline and Airline's program partners	● Marketing purposes ● To facilitate Member participation ● To assess applications ● To award points ● To confirm eligibility for products and services ● To enhance and tailor the service ● To generate consumer insights
Supermarket	● Personal details (name, addresses, telephone numbers, age and gender) ● Customer reference number or loyalty card number ● Response to offerings (eg membership of clubs and loyalty programs, financial services products, mobile applications) ● Any rewards and redemption details ● Connections to others who Supermarket may collect personal information from (e.g. family members linked to a loyalty program membership) ● What, how and when products are bought ● Expression of interest in buying from Supermarket ● Stated or likely preferences (e.g. particular products or promotions) ● Health information (for optical or insurance services; public liability issues) ● Secure financial information (debit/credit card) ● Accessing data from other sources about likely preferences and interests (eg when visiting Supermarket's websites, social media pages or mobile applications or click on advertisements - that information is collected as cookies)	● To learn of likely preferences to promote goods and services in a targeted way ● To assist in investigation complaints and enquiries

Organisation	Type of personal information collected (as per company's privacy policy)	What information is used for (as per company's privacy policy)
Online Clothing Store	● Name ● Contact details ● Identification information ● History records of communications and correspondence with Online Clothing Store ● Details or history of preference, interests and behaviour in relation to transactions, products, services and activities on the website ● Computer IP address ● Browser type ● Webpage visited before navigating to Online Clothing Store site ● Pages within Online Clothing Store's website that are visited ● The time spent on those pages, items and information searched on the Site including access times, dates and other statistics	● To provide products and services ● To communicate with the user, including about products and services, competition results, special offers and events that may be of interest ● To answer customer queries and to provide information or advice ● To create orders, transaction records, agreements for the sale of products or services, accounts, tax invoices or receipts ● To improve or develop products and services ● To perform research and analysis ● To carry out administration, marketing, planning, fraud and loss prevention activities, procurement, product and service development, quality control etc ● To comply with laws or regulations
Bank (Personal Banking)	● Name ● Date of birth ● Phone number ● Annual income and other financial details ● Credit history ● Email address ● Place of work ● Tax file number ● Transaction history ● Information provided when opening an account ● Completed application forms ● Correspondence	● To provide products and services and support ● Administration of the account ● For operational and legal purposes ● Marketing ● Preventing or investigating any actual or suspected fraud, unlawful activity or misconduct ● To establish tax status

Organisation	Type of personal information collected (as per company's privacy policy)	What information is used for (as per company's privacy policy)
	● Use of website or branches ○ Credit reporting bodies ○ Other credit providers ○ Organisations that Bank has an arrangement with to jointly offer products and/or an alliance with to share information for marketing purposes ○ Related entities ○ Marketing companies ○ Brokers and other parties who have referred the customer to Bank ● How the website is used and how other websites are used (cookie information) ● Sensitive information (where needed)	
Bank (Credit)	Information collected and stored to provide to credit reporting bodies: ● Account identification information ● Type of personal credit (eg credit cards, home loans or personal loans) ● Amounts borrowed ● If and when repayments are made including up to 24 months of repayment history ● Dates personal credit account was opened and closed ● Applicable credit limit ● Any fraud offences or other serious credit infringements May request credit reporting bodies provide to the Bank: ● Overall credit score ● Other credit information	● To confirm identity ● To assess applications ● To design, manage, price and provide products and services ● To manage the client relationship ● To minimise risks and identify or investigate fraud and other illegal activities ● Correspondence ● To improve services ● To comply with laws ● Operational purposes ● Improved customer service
Health Insurer	● Completion of application at a retail centre or online ● Details provided over the phone ● Information about claims made ○ Date ○ Amount paid	● Processing applications ● Administering policy ● Investigating, assessing and paying claims ● Processing payments

Organisation	Type of personal information collected (as per company's privacy policy)	What information is used for (as per company's privacy policy)
	○ Service type ○ Description of service ○ Healthcare provider ○ Information about treatments received ● Name, address, telephone and email contact details ● Gender, date of birth and marital status ● Billing details ● Records of any correspondence including system notes and voice recordings of telephone conversations ● Census and statistical information ● Current and previous products ● Changes of cover, cancellations or suspensions of policy ● Medicare number ● Details of registration for Australian Government Rebate on private health insurance and income tier for rebate purposes ● Participation in health management programs or other health related services provided by Health Insurer ● Employer details	● Correspondence ● Identifying suitable products ● Conduct health management programs ● To answer queries ● To conduct quality assurance activities and research of health and wellness programs ● For administration, training, accounting, auditing and information technology purposes ● To practice effective risk management ● To prevent fraud ● To monitor, price and evaluate products and services ● To resolve complaints; ● To conduct market research and analysis ● To comply with laws and regulations ● To fulfil marketing promotions
Telecommunications Provider	● Name, date of birth, contact details (including address, email address, phone number or mobile telephone number) ● Occupation ● Driver's licence or passport number ● Telecommunications Provider account information (PIN, username, password) ● Financial information (credit card or bank account) ● Financial and credit information (income details, payment history, credit history, service history) ● Information about products and services (hardware model, operating system version, unique device and service identifiers, device status,	● For administration ● To prevent fraud ● To ensure network security ● For communications ● To improve goods and services ● For development and analysis through analysing data trends ● Direct marketing ● Compliance

Organisation	Type of personal information collected (as per company's privacy policy)	What information is used for (as per company's privacy policy)
	serial numbers, settings, configuration and software, mobile network information) ● Information about how products and services are used ○ Network usage (time and duration of communications, operation of the equipment, services and applications used on the network) ○ How services are used to access the internet (eg websites visited) ○ Location or location of the devices when using products or services ○ Information for verification purposes (eg fingerprints or voice patterns) ● Technical information about products and services (network performance) ● Health information (where needed for priority assistance services) ● Centrelink customer reference number (eg for pensioner discount)	
Online Payments Provider	● Cookie data ○ Pages accessed ○ IP address ○ Device identifiers ○ Type of operating system used ○ Location ○ Mobile network information ○ Standard web log data (e.g. browser type; traffic to and from site) ● Contact information (name, address, phone number and email address) ● Financial information (bank account numbers, credit/debit card numbers) ● Date of birth ● Drivers licence number/ other ID documents ● Credit reports	● To provide services ● For customer support ● To process transactions and to send notices in relation to transactions ● To resolve disputes, collect fees and troubleshoot problems ● To investigate or prevent potentially illegal activities ● To enforce the User Agreement ● To develop an understanding of customer satisfaction, expectations and usage ● To customise, measure and improve services ● To deliver targeted marketing,

Organisation	Type of personal information collected (as per company's privacy policy)	What information is used for (as per company's privacy policy)
	● If authorised, information from third parties such as social media sites	service update notices and promotional offers ● For communications ● To compare information for accuracy and verification ● For data analytics ● For consensual purposes ● As required by law
Media Company	● Registration information (name, delivery or postal address, email address, gender and birthday) ● Public information and posts (comments or content posted online to Media Company's services—e.g., name, user name, comments, likes, tweets, status, profile information and picture(s)) ● Information from third party social media (if accessing a Media Company service through a third party social media service; could include user name, profile picture, email address, followers or friends list, or any other public information) ● Activity information - Cookies and other technologies ○ IP address ○ Browser type ○ Software/hardware information ○ Unique device identifier ○ Geolocation data ○ Other transactional information	● To deliver relevant advertising and services ● For research and data analysis ● To fulfill administrative functions (e.g., billing, credit and account management) ● To enter into contracts with the user or third parties ● To measure and improve Company Services and their individual features ● To improve user experience by delivering targeted content (including editorial, marketing and advertising) ● For other marketing and client relationship purposes ● To allow users to comment on content, and participate in games, competitions, or rewards programs ● For customer support ● To respond to enquiries
Media Company	● Name ● Contact details (address, phone number, fax, email address)	● To arrange, conduct and promote media activities (e.g., production,

Organisation	Type of personal information collected (as per company's privacy policy)	What information is used for (as per company's privacy policy)
	● Birth date ● Gender ● Interests and viewing of programs and services ● Records of transactions ● Completed surveys or questionnaires ● Communications ● IP address ● Type of operating system used ● Domain name of ISP ● Software and hardware attributes ● Webpage requested ● Media Company cookies ● Third-party cookies (including third-party tracking service providers, third party advertisers and ad network companies, demand side platforms and server side platforms) ○ Behavioural data for online advertising ○ Data for interest-based advertising ● Audience ratings information and anonymous viewing data	broadcasting, and publishing) ● Establish and administer access to services ● To provide products and services ● Identifying and displaying targeted content ● For product and service referrals ● For targeted behavioural or interest-based advertising ● To improve services and conduct research ● For communications ● For internal auditing and administration ● For marketing purposes