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

google.com

22 January 2022

Attorney General's Department
Robert Garran Offices
3-5 National Circuit
BARTON ACT 2600

BY EMAIL: PrivacyActReview@ag.gov.au

Thank you for the opportunity to provide feedback on the recently published Discussion Paper that develops responses to the Issues Paper and seeks further feedback on potential changes to the *Privacy Act (Cth)* 1988 (the "Act").

As stated in our submission on the Issues Paper, Google is supportive of the review and update of the Act and we will therefore focus our comments in this submission on questions and concerns with a small number of the potential changes outlined in the Discussion Paper.

Definition of personal information

The goal of any changes to the definition and scope of 'personal information' should be to encourage the use of less-identified data wherever possible. To this end, defining which data types are not captured by this definition is almost as important as defining what is captured. We suggest that household data, aggregated data, publicly available data and any other sources of data that are not about a specific individual or device should be explicitly excluded from this definition.

We would welcome the opportunity for discussion about the inclusion of inferred or generated data within the definition of personal information. There is a wide variety of data that is being inferred through machine learning that does not use personal information nor does it increase the likelihood of being able to identify an individual. For example, contextual advertising relies on inferences drawn from an unidentified person consuming content that relates to a specific

issue or topic (e.g. an article on smh.com.au about a new film release) and then serving an ad that relates to that content (e.g. a cinema ad). There is no personal information being collected, used or shared to serve this ad and we would like to better understand the policy intention here.

With respect to the requirement that personal information be anonymised before it can be excluded from the Act, we note that certain responsibilities needing to be carried out by entities regulated under the Act cannot be performed on pseudonymous data (e.g. portability, right to access / object). We suggest that pseudonymous data also be considered in this context.

Flexibility of the APPs / Code development

We don't have any concerns in principle with the proposal that the Attorney General can direct the Commissioner to develop / impose an APP code without first requesting industry to develop in cases of emergency or where in the public interest. However we would like to see a codified threshold test, including the requirement to solicit and consider public comments, for how the public interest is measured and applied in these exigent circumstances.

Notices of collection of personal information / Consent

We are pleased to see the acknowledgement within the Discussion Paper of the need to avoid a proliferation of notices in order to avoid consent fatigue and support an explicit requirement that notices under APP5 be clear, current and understandable. Google has dedicated significant resources over the years to evolving the presentation of privacy information in a manner that is accessible and increasingly contextual and we see tremendous scope for innovation in the way in which entities present this information.

While we appreciate the desire for standardisation, we welcome further discussion on this matter to ensure that entities retain the flexibility to design and convey notices and collect consent in the most appropriate manner based on their specific service. For example, the delivery of information to inform a consent choice in the context of a search engine is very different to how you might request consent within a mapping app.

Additional protections

With respect to the proposed distinction between primary and secondary purposes, we think this warrants more discussion and consideration. We suggest that secondary purposes "needed to support" the primary purpose is perhaps too limiting a distinction. We think it helpful to consider what might reasonably be expected from a customer beyond a primary purpose for data collection. It might also be useful to further discuss introducing the concept

of legitimate purposes, as exist under the European General Data Protection Regulations (GDPR).

Restricted and prohibited acts and practises

We prefer option 1 of the two options identified in this section of the Discussion Paper. Option 1 places clear responsibility on the regulated entity to acknowledge these higher risk practises and give careful thought to how these risks can be minimised. This is preferable to placing the burden on the customer to self-manage.

Default settings

Both of the default setting options set out in the Discussion Paper start from the premise that the most restrictive setting is optimal for all customers. In our experience, customers have different thresholds and tolerances relating to the sensitivity of their personal information and data about them. Requiring specific default settings also ignores a third option of asking customers to make a choice without having set any default. The emphasis here should be on granting as much control over data to customers as possible. Of the two options presented, we prefer option 2.

Children and vulnerable adults

We appreciate the unique circumstances of children and vulnerable adults and acknowledge that the Act has protected all Australians, including children and vulnerable adults, since its inception. Requiring age verification and parental consent for data collection, use and disclosure relating to children under 16 is a significant change in policy and we appreciate that this process is facilitating a considered and inclusive whole-of-society discussion on the matter.

Many countries have grappled with the appropriate age of consent for children and have taken different approaches, ranging between 13 - 18. We suggest that the appropriate age for Australian children sits between 13-14 and that stricter default settings could be applied to teenagers aged between 14-18.

Turning to the concept of age verification, we commend the work carried out by the UK Information Commissioner's Office (ICO) on age assurance[1] in the context of the UK Age Appropriate Design Code. The ICO has adopted the use of the term 'age assurance' to refer to a spectrum of four approaches to determining or inferring age each with their own strengths and weaknesses, including how privacy invasive each method is. The four approaches are;

[1] ICO opinion on Age Assurance for the Children's Code published 14 October 2021

1. Age verification;
2. Age estimation;
3. Account confirmation; and
4. Self declaration.

The UK ICO urges organisations to consider a proportionate assessment of the risk to children and stresses the need to adopt the most proportionate, less privacy invasive approaches where possible.

No age assurance mechanism is 100% accurate, and the more accurate the mechanisms are required to be, the more intrusive they are likely to be. Highly prescriptive "age verification" requirements tend to lead to companies having to collect more information (potentially including sensitive information) about all individuals in order to determine if they are a child. Age assurance models should follow a risk-based assessment and be implemented in a proportionate way, balancing the need for accuracy with the risk of limiting rightful access to information and impact on users' privacy. Age assurance measures should complement parental tools that help put parents at the centre of deciding what is best for their children and families. And they should build on robust product design and clear policies to ensure that users, and children in particular, have a safer and more enriching experience.

Irrespective of where we collectively settle on the age of consent, we therefore suggest that any new age verification policies apply to new customers only (i.e. do not apply retroactively) and are limited to high risk data processing with less intrusive forms of age assurance deployed for lower risk processing.

Parental consent methods should be inclusive of the reality that not all people under the age of consent have parents / guardians and that not all adults have access to the same methods of verification. (e.g. credit cards are not available equally across demographics). Perhaps the Office of the Australian Information Commissioner could be tasked with producing guidance on suitable methods for Australia? We also note that the eSafety Commissioner has been tasked by the Government with developing a roadmap for age verification (due by December 2022) and we suggest that any efforts to advance thinking in the context of the review of the Act be done in conjunction with the consultative and thorough work being carried out by the eSafety Commissioner.

Right to object

We are comfortable with the proposed right to object, and strongly support the opportunity for an entity to inform the individual of the consequences of their objection. This right will need to be scoped in such a way that does allow time for entities to respond and for individuals to consider that response before the exercise of their right is confirmed.

Right to erasure

We are also comfortable with this proposed right and suggest that the scope of data subject to the erasure be limited to data provided by the customer and logs that reflect account access and transactions.

Direct marketing, targeted advertising and profiling

We note that beyond the heading of this section of the Discussion Paper, the term "direct marketing" is used apparently as an all encompassing term to include targeted advertising and profiling. We welcome confirmation that this interpretation is correct. We already offer the ability to turn personalised advertising off across Google and third party platforms (where Google serves the ads), however we have observed that some customers consider turning personalised advertising off to mean that they will cease seeing any advertisements (personalised or not). It might be worth highlighting that a right to object to personalised advertising does not mean that no advertisements will be served thereafter and that rather it simply means that advertising will not be tailored to a person's interests.

The reference to "influencing behaviour or decisions" suffers from definitional ambiguity and suggests a sinister intention. The experience of our users comes first, which is why Google seeks only to show ads that are helpful and relevant to people. Over time, our investments in ad quality systems have led to better, more relevant and major improvements in the overall user experience. Furthermore, one could argue that all forms of advertising are seeking to influence behaviour or decisions and this could have unintended consequences for advertising funded platforms. Using a mapping app to guide navigational decisions based on traffic congestion or public transport disruptions has a clear benefit to customers that is not recognised within this section of the Discussion Paper. We look forward to discussing this in more detail.

Privacy Preserving Technologies and Innovations

We strongly support the inclusion of incentives in new provisions of the Privacy Act that incentivise companies who seek to evolve commercial practises in ways that are more privacy preserving. As technology used for digital commercial practises evolve, a variety of protocols, processes, and protections that can be built-in at a technical level to help safeguard individual privacy and enhance data protection are being developed, which aim to make the internet safer while unlocking the incredible potential of data-driven innovation. Through the use of privacy preserving technologies and innovations, companies, researchers, and governments can develop meaningful, useful insights and services while preserving individual privacy, resulting in a positive impact on society. Incentivising the creation and use of these technologies will result in swift improvements to user privacy, which are market driven.

Organisational accountability

We are comfortable with the proposal to "Amend APP6 to expressly require entities to determine, at or before using information for a secondary purpose, each of the secondary purposes for which the information will be used or disclosed and record those purposes" and suggest that this amended APP6 is drafted consistently with the purpose limitation clause in the European General Data Protection Regulation Article 5(1)(b).

Overseas data flows

We note the proposal to "Remove the informed consent exception in APP8.2B (exemption to comply where consent is given to overseas transfer)" and welcome further clarification on the policy intention for removing this exception, noting that informed consent is a common prerequisite for data transfers.

Data controller / data processor

We note the Issues Paper touches briefly on the concept of data controller/data processor and would encourage and welcome more detailed consideration of this concept as part of the review process. The introduction of a data controller/processor framework in Australia would align with global privacy frameworks (ISO, GDPR, US privacy regulations), simplifying compliance obligations for controllers and processors, and providing clearer engagement/escalation and enforcement paths for individuals and regulators.

A controller/processor framework would also capture how businesses engage with each other, assign appropriate accountability based on the relationship to the user, and role in making processing decisions. Typically local companies act as data controllers and therefore they define the purpose and means of the processing of personal data. This gives more control over user data to local companies. Cloud providers typically act as data processors and process data based on the data controller's instructions.

Cross-border privacy rules and domestic certification

The necessity for the introduction of a domestic certification scheme should be subject to further detailed consideration. We previously recommended that the Act be updated to encourage global interoperability, including by recognising the same or substantially similar grounds for transfer as the GDPR short of adequacy (e.g., contractual clauses, consent, necessary for contract), and/or explicitly acknowledging the intention to achieve interoperability with relevant provisions of GDPR.

We reiterate that the adoption of, or alignment with, existing global certifications should be preferred to minimise the compliance burden on organisations, and enable harmonisation with obligations in other markets, rather than imposing a domestic certification which may overlap, or in part duplicate, other existing frameworks.

Enforcement

We welcome further discussion about how an industry funded model would work. Is the intention that all regulated entities contribute funding or that only those entities that are the subject of an enforcement action or investigation provide funding?

We are also interested to hear more about the proposal for encouraging additional regulatory models. Clearly the OAIC already has a complaint handling team comprised of privacy subject matter experts. Is this team overburdened? We are open to exploring additional models, but would appreciate a better understanding of the problem that needs to be solved.

Direct right of action

We welcome the suggestion that a complainant must have lodged a complaint with the OAIC or an external dispute resolution scheme before initiating a direct action, however we are concerned that the proposal permits a complainant to launch a direct action without participating in a conciliation, which is a standard component of the existing complaint handling process administered by the OAIC. We suggest that requiring at least an attempt to resolve a dispute through alternative forms of dispute resolution is an appropriate pre-requisite for launching a direct action. We are also interested to discuss whether a serious harm threshold ought to be met before a direct right of action can be initiated.

Statutory tort of privacy

We appreciate the range of options being considered to address the issue of a statutory tort. Option 2 is interesting but we wonder whether courts are well equipped, both in terms of knowledge / expertise as well as capacity, to develop a body of precedent on the scope and application of any minimalist tort. We have seen, in the context of defamation by way of example, that courts have struggled to apply more traditional legal principles to emerging technologies.

Location data as sensitive data

While not specifically canvassed as a proposal, there is a question raised in the Discussion Paper about expanding the definition of sensitive data categories to include location data. In considering whether location data could / should be treated as sensitive data, this should

depend on how identifiable the individual is and the degree to which the collection of location data would naturally be expected by the individual. For instance, location data that positions someone within a suburb or postcode but not a specific address should not be considered personal information, let alone a sensitive data category. For most advertising use cases, location data is no more specific than a geographic area of at least 3 sq km and containing at least 1000 users.

Once again, we appreciate the opportunity to contribute to this important discussion. Please be in touch with any questions about this submission or to discuss any of the issues raised in more detail.

Yours sincerely,

Samantha Yorke

Government Affairs and Public Policy

Google Australia