The Australia Institute
Research that matters.
Centre for Responsible Technology

Blinding Big Brother: Overhauling Australia's Privacy Act for the Internet age

Submission to the Privacy Act Review Discussion Paper

Jordan Guiao
Research Fellow, Centre for Responsible Technology

December 2021

About The Australia Institute

The Australia Institute is an independent public policy think tank based in Canberra. It is funded by donations from philanthropic trusts and individuals and commissioned research. We barrack for ideas, not political parties or candidates. Since its launch in 1994, the Institute has carried out highly influential research on a broad range of economic, social and environmental issues.

About the Centre for Responsible Technology

The Australia Institute established the Centre for Responsible Technology to give people greater influence over the way technology is rapidly changing our world. The Centre will collaborate with academics, activists, civil society and businesses to shape policy and practice around network technology by raising public awareness about the broader impacts and implications of data-driven change and advocating policies that promote the common good.

Our philosophy

As we begin the 21st century, new dilemmas confront our society and our planet. Unprecedented levels of consumption co-exist with extreme poverty. Through new technology we are more connected than we have ever been, yet civic engagement is declining. Environmental neglect continues despite heightened ecological awareness. A better balance is urgently needed.

The Australia Institute's directors, staff and supporters represent a broad range of views and priorities. What unites us is a belief that through a combination of research and creativity we can promote new solutions and ways of thinking.

Our purpose – 'Research that matters'

The Institute publishes research that contributes to a more just, sustainable and peaceful society. Our goal is to gather, interpret and communicate evidence in order to both diagnose the problems we face and propose new solutions to tackle them.

The Institute is wholly independent and not affiliated with any other organisation. Donations to its Research Fund are tax deductible for the donor. Anyone wishing to donate can do so via the website at https://www.tai.org.au or by calling the Institute on 02 6130 0530. Our secure and user-friendly website allows donors to make either one-off or regular monthly donations and we encourage everyone who can to donate in this way as it assists our research in the most significant manner.

Level 1, Endeavour House, 1 Franklin St
Canberra, ACT 2601
Tel: (02) 61300530
Email: mail@tai.org.au
Website: www.tai.org.au
ISSN: 1836-9014

Summary

The Privacy Act is a critical piece of legislation designed to protect Australians' right to privacy. Since its inception in 1988 it has not been properly updated to account for the significant changes the internet has made to individual privacy. Moreover, it was never designed to counter the business models of companies like Google and Facebook that are powered by vast collection and processing of data and personal information.

The Australia Institute's Centre for Responsible Technology welcomes the opportunity to make a submission to this review and put forward the following recommendations:

- Ensure the appropriate level of technical information is captured as part of the updates to the relevant areas of 'personal information'. Looking at what Google captures alone will show extensive technical and inferred information, including location history, interest and hobbies and third party tracking.
- Move away from 'notice and consent' models which have proven to be ineffectual, and place the regulatory burden on platforms rather than individuals, considering requirements such as:
    - **Purpose limitations,** making sure that data collection is restricted to the explicit and singular purpose for which it was consented to, with no secondary usage or extra data transfer.
    - **Data separation,** limiting the sharing of user data between a company's different products. For example, the location data collected by Google Maps with user consent could not be shared with Google Search and used to target advertising at the user.
    - **Data minimisation,** only capturing the minimal amount of data.
- Apply mandatory additional requirements for high-risk activities like a Data Protection Impact Assessment for large scale data collection and processing.
- Create red lines and additional restrictions for sensitive data like biometrics and facial recognition, and where possible, ban this activity.
- Have privacy by default features on all relevant activities.
- Enable stronger user controls, including the right to object and the right to erasure.
- Place responsibility on platforms, rather than individuals, by encouraging privacy by design and other privacy-friendly frameworks.
- Evolve the Office of the Australian Information and Privacy Commissioner's (OAIC's) capabilities to meet these new demands, including additional penalties like multi-level privacy penalties, a new Ombudsman and/or Deputy Commissioner, and a new statutory tort for privacy breaches.

Introduction

The Internet has impacted Australians in far-reaching ways. Not the least of which is to individual privacy. Online platforms like Google allow users to see into different neighbourhoods from across the world and gather data on everywhere users have been (both online and offline), Meta/Facebook know all about people's networks, the things shared between them, and the public's diverse interests and hobbies. Online platforms may know more about individuals than they know about themselves, as these companies are able to harvest personal digital data from devices, locations, purchases, viewing habits,[1]and even biometric data[2] and bodily functions[3] in real time.

The Privacy Act which governs Australians' overall privacy, including online, has not been suitably updated to account for these vast changes and capabilities. Developed in 1988 the Privacy Act did not see the internet coming. There have been different updates to address specific needs and some expansion in scope since inception. These include the creation of a dedicated Privacy Commissioner in 2000 and its integration into the Office of the Australian Information Commissioner (OAIC) in 2010. The coverage of the Act was extended to some private sector organisations since 2001, and standards were developed on the collection, access and storage of personal information. More significant reforms were conducted in 2014 to include the Australian Privacy Principles and new enforcement powers for the Information Commissioner, and also in 2018 with the addition of the Notifiable Data Breaches scheme for protection against intentional or unintentional release or access of secure information without consent and into an untrusted environment.[4] While incremental updates have been conducted to date, there needs to be a wholesale update to account for the disruptive and expansive privacy considerations brought about by the internet.

The Australia Institute's Centre for Responsible Technology welcomes the opportunity to make a submission to this critical review. This submission addresses the following proposals/questions from the discussion paper:

[1] Smith (2020), *Google collects a frightening amount of data about you. You can find and delete it now,* https://www.cnet.com/tech/services-and-software/google-collects-a-frightening-amount-of-data-about-you-you-can-find-and-delete-it-now/

[2] Shiaeles (2021), *Facebook will drop its facial recognition system – but here's why we should be spectical,* https://theconversation.com/facebook-will-drop-its-facial-recognition-system-but-heres-why-we-should-be-sceptical-171186

[3] Williams (2021), *Google now owns Fitbit: What it means for your fitness data privacy,* https://www.forbes.com/sites/andrewwilliams/2021/01/14/google-now-owns-fitbit-what-it-means-for-your-fitness-data-privacy/?sh=5ea2c2b539e1

[4] Office of the Australian Information Commissioner (2021), *History of the Privacy Act,* https://www.oaic.gov.au/privacy/the-privacy-act/history-of-the-privacy-act

- In practice, what types of information would the proposed definition of personal information capture which are not presently covered?
- Consent is to be defined in the Act as being voluntary, informed, current, specific, and an unambiguous indication through clear action.
- Standardised consents should be considered in the development of an APP (Australian Privacy Principles) code, such as the OP (Online Privacy) code, including standardised layouts, wording, icons, or consent taxonomies. Consumer comprehension testing would be beneficial to ensure the effectiveness of the standardised consent.
- Define a 'primary purpose' as the purpose for the original collection, as notified by the individual. Define a 'secondary purpose' as a purpose that is directly related to, and reasonably necessary to support the primary purpose.
- Would the proposed definition of a secondary purpose inadvertently restrict socially beneficial uses and disclosures of personal information, such as public interest research?
- Would the introduction of a specified restricted and prohibited practices be desirable?
- Should restricted practices trigger a requirement for APP entities to implement additional organisational accountability measures, or should individuals be provided with more opportunities to self-manage their privacy in relation to such practices?
- What acts and practices should be categorised as a restricted and prohibited practice, respectively?
- Should prohibited practices be legislated in the Act, or developed through Commissioner-issues guidelines interpreting what acts and practices do not satisfy the proposed fair and reasonable test, following appropriate public consultation?
- Introduce pro-privacy defaults on a sectoral or other specified basis. Option 1 – Pro-privacy settings enabled by default, where an entity offers a product or service that contains multiple levels of privacy settings, an entity must pre-select those privacy settings to be the most restrictive. This could apply to personal information handling that is not strictly necessary for the provision of the service, or specific practices identified through further consultation.
- An individual may object or withdraw their consent at any time to the collection, use or disclosure of their personal information. On receiving notice of an objection, an entity must take reasonable steps to stop collecting, using or disclosing the individual's personal information and must inform the individual of the consequences of the objection
- In light of submitter feedback, should a 'right to erasure' be introduced in the Act?
- Introduce further organisational accountability requirements into the Privacy Act, targeting measures to where there is the greatest privacy risk: Amend APP 6 to expressly require APP entities to determine, at or before using or disclosing personal information for a secondary purpose, each of the secondary purposes for which the information is to be used or disclosed and to record those purposes.

- Create tiers of civil penalty provisions to give the OAIC (Office of the Australian Information and Privacy Commission) more options so they can better target regulatory responses, including: A new mid-tier civil penalty provision for any interference with privacy, with a lesser maximum penalty than for a serious and repeated interference with privacy. A series of new low-level and clearly defined breaches of certain APPs with an attached infringement notice regime.
- Alternative regulatory models Option 2 – Create a Federal Privacy Ombudsman that would have responsibility for conciliating privacy complaints in conjunction with relevant EDR (External Dispute Resolution) schemes. Option 3 – Establish a Deputy Information Commissioner – Enforcement within the OAIC.
- Introduce a statutory tort for invasion of privacy as recommended by the ALRC (Australian Law Reform Commission) Report 123.
- Establish a Commonwealth, state and territory working group to harmonise privacy laws, focusing on key issues.

Privacy proposals

TECHNICAL INFORMATION IS PERSONAL INFORMATION

Big Tech companies like Google collect vast amounts of personal information, data that powers its products and services. Importantly, most people would not be aware of the extent to which their information is being captured.

Including technical information and inferred information in consideration of personal information is critical in protecting the privacy of Australians.

Companies like Google and Meta/Facebook offer some ability for individuals to download and collect their data but this typically only provides superficial or volunteered information, and not the metadata or technical information being captured.

Google alone conducts extensive data collection through first party as well as third party data, including:

Data from having a Google account (e.g. Gmail, Google Docs, Google Drive)

- Name
- Date of birth
- Gender
- Email
- Phone number

Data from using any of Google's many consumer products and services

- Search history from Google Search
- Location history from Google Maps
- Movement data from Google Maps
- Interest and hobbies from YouTube
- Viewing history from YouTube
- Interest and hobbies from Gmail
- Interest and hobbies from Blogger

Data from use of Google devices, such as Android phones and Google Home and Nest, and through using Google apps on smartphones

- IP address
- Network connection information
- Location information
- Device attributes
- Device signals
- Home smoke alarms through Google Home and Nest

- Indoor and outdoor cameras through Google Home and Nest
- Thermostats through Google Home and Nest
- Doorbells through Google Home and Nest

Payment data collected through Google Pay

- Purchase history
- Credit Card information
- Debit Card information
- Billing address

Third party data tracking

- 80% of the most popular 1,000 websites in Australia had Google tracking
- 91% of the most popular 1,000 apps had Google tracking[5]

The depth and breadth of technical information being captured should be accounted for in the updates to the Privacy Act.

BEYOND 'NOTICE AND CONSENT'

There are clear limitations with the notice and consent model that are now widely acknowledged.[6][7][8] The ACCC Digital Platform Inquiry,[9] and the explanatory paper for the Online Privacy Bill[10] have called out that current notice and consent frameworks often use overly cumbersome privacy notices, which are complex and take too long to read, and that most people therefore do not read them. Most notices often use jargon heavy and ambiguous language which are not easily understood.

Even if notices become easy to understand and clearly lay out how personal information is collected, the sheer scale and volume of data processing online mean that individuals would

[5] ACCC (2020), *Digital Advertising Services Inquiry interim report*, pg. 65

[6] Johnston (2020), *Re-thinking transparency: If notice and consent is broken, what now?,* https://www.salingerprivacy.com.au/2020/05/29/re-thinking-transparency/

[7] Park (2020), *How "Notice and Consent" Fails to Protect our Privacy,* https://www.newamerica.org/oti/blog/how-notice-and-consent-fails-to-protect-our-privacy/

[8] King, Katsanevas, Flanagan (2021), *Online privacvy notices don't work. Here are 9 alternatives,* https://www.weforum.org/agenda/2021/04/online-privacy-notices-are-a-farce-here-s-an-alternative/

[9] ACCC (2019), *Digital platforms inquiry – final report*, https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report

[10] Australian Attorney-General's Department (2021), *Explanatory paper, Privacy Legislation Amendment (Enchancing Online Privacy and Other Measures) Bill 2021,* https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/user_uploads/online-privacy-bill-explanatory-paper.pdf

have a very difficult time consenting to each specific data exercise across multiple products and services.

Rather than placing the burden on individuals, there should be more emphasis on platform responsibility and 'privacy by design' features, with privacy friendly restrictions and architecture which limit data collection in the first instance. Privacy models should develop the following features, which will reduce the need and responsibility on active consent requests:

- Purpose limitations, making sure that data collection is restricted for the explicit and singular purpose to which it was consented to, and no secondary usage or extra data transfer is conducted.
- Data separation, limiting the ability for companies to share user data between its different products and services (e.g. consenting to use Google Maps does not mean Google can use that location data to target users using Google Search).
- Data minimisation, only capturing the minimal amount of data.

RED LINES

Many issues have come to light with the large-scale collection and processing of data, particularly from Big Tech companies like Google and Meta (Facebook). At scale, these issues have contributed to decreased trust in institutions and attacks against democracy,[11] civil instability,[12] and physical harms and violence.[13] These stems from the unfettered access many Big Tech companies have in data collection and processing. Therefore, there should be additional restrictions and limitations placed on these practices.

The European Union's General Data Protection Regulation (GDPR) requires that a Data Protection Impact Assessment (DPIA) be mandatory for all data processing activities which are:

1) Systemic and extensive with significant effects
2) Large scale use of sensitive data
3) Public monitoring[14]

[11] Anderson & Rainie (2020), *Concerns about democracy in the digital age,* https://www.pewresearch.org/internet/2020/02/21/concerns-about-democracy-in-the-digital-age/

[12] Timberg et. al. (2021), *Inside Facebook, Jan.6 violence fuleed anger, regret over missed warning signs,* https://www.washingtonpost.com/technology/2021/10/22/jan-6-capitol-riot-facebook/

[13] Mozur (2018), *A genocide incited on Facebook, with posts from Myanmar's military,* https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html

[14] UK Information Commissioner's Office (2021), *When do we need to do a DPIA?,* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/

A similar requirement should be observed as part of the Australian Privacy Act. This type of assessment or analysis should account for the many issues that are caused by large scale data processing, and additional mitigation and even penalties should be explored at the end of the assessment.

Further, the sensitive area of biometric data should be a specific area of focus. The Australian Human Rights Commission have called for a moratorium on biometric harvesting like facial recognition technology due to the sensitivity and its potential for rampant and dangerous abuses.[15]

Biometric technology contains many issues. They are often black boxes with proprietary intellectual property held by private companies. There are issues with transparency and quality control and errors.[16] Facial recognition technology continue to have severe limitations and errors in certain practices (such as the 'one-to-many' methodology), resulting in false positives and misidentification with very damaging results.[17] Biometrics have known biases against women and people of colour[18] and have been used as surveillance tools to prosecute minorities.[19] In general, biometric scanning normalises surveillance culture, which fundamentally breaches an individual's right to privacy.

High-risk and large-scale data processing should therefore at a minimum be subject to additional restrictions, limitations and analysis, and in the case of sensitive areas like biometrics, should be banned where possible.

PRIVACY BY DEFAULT

By observing the principles of purpose limitations and data minimisation, options for privacy features should be at its most restrictive by default. The power of the default setting is a well-known phenomenon[20] and moving towards a privacy by default culture would go towards protecting the privacy of Australians.

[15] Australian Human Rights Comission (2021), *Human Rights and Technology Final Report*

[16] Wiggers (2021), *Bias persists in face detection systems from Amazon, Microsoft, and Google,* https://venturebeat.com/2021/09/03/bias-persists-in-face-detection-systems-from-amazon-microsoft-and-google/

[17] Castelvecchi (2021), *Is facial recognition too biased to be let loose?* https://www.nature.com/articles/d41586-020-03186-4

[18] Ibid.

[19] Fernando (2020), *Advances in facial recognition technology could amplify the persecution of minorities, AI experts warn,* https://www.sbs.com.au/news/advances-in-facial-recognition-technology-could-amplify-the-persecution-of-minorities-ai-experts-warn/da16ed2b-daa4-4b04-80c7-89b730388f1b

[20] Mandl, Felfernig, Tiihonen, Isak (2011), *Status quo bias in configuration systems*, https://www.researchgate.net/publication/221047754_Status_Quo_Bias_in_Configuration_System

USER CONTROL

While the responsibility of privacy protection should be placed largely in the hands of digital platforms, there should be suitable user management controls to allow individuals to have agency over their own data.

This is exemplified in the 'right to object' and the 'right to erasure' proposals

The right to object has strong precedents in the California Consumer Privacy Act (CCPA) where there is the ability for users to opt-out of the sale of their personal information.[21]

This feature has been proven to be very popular with users, as demonstrated in the case of Apple's iOS 14.5 update. As part of the new operating system update, Apple prompted users with a choice of whether they wish to be tracked, and an overwhelming majority (75%) of users declined.[22]

The right to erasure/right to delete has precedents in both the CCPA and the GDPR.

A 'right to erasure' action would empower individuals and give them agency over their data management, especially as data processing online increasingly becomes more complex and harder to keep track of. There are many reasons why personal information may be considered private, outdated, or out of context. Minors and young people in particular should also be protected from permanent digital records of their activities before they are legal adults.

During the rollout of the GDPR, the UK's Department for Culture, Media & Sport commissioned a report which sought to quantify the economic benefits arising from greater consumer trust and agency in the digital economy. The report looked specifically at the benefits of individual control, such as the 'right to erasure', and conducted a combination of quantitative and qualitative surveys, online forums, in-depth interviews and literature reviews.

The 'right to erasure' was determined as having a range of benefits including ending harmful use of data, more accurate data and cost savings as part of the EU's GDPR rollout.[23] Figure 1

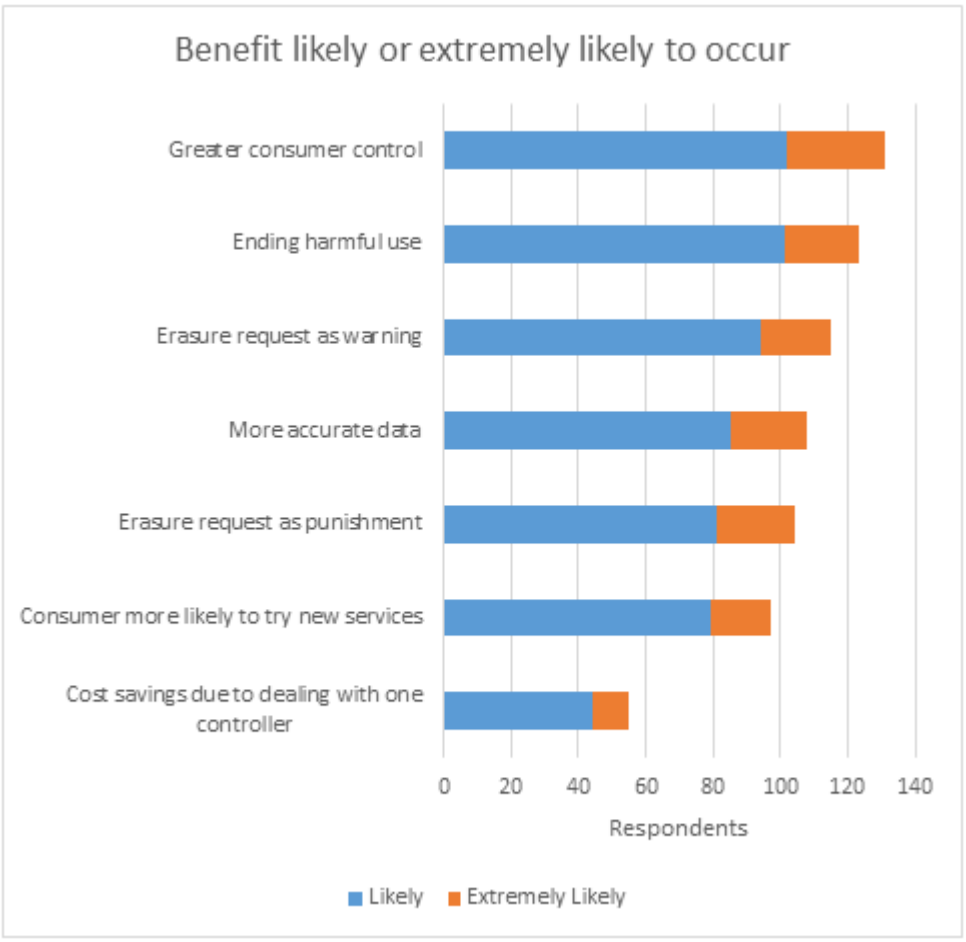
[21] Bonta (2021), *California Consumer Privacy Act (CCPA),* https://www.oag.ca.gov/privacy/ccpa

[22] Wagner (2021), *Facebook users said no to tracking. Now advertisers are panicking,* https://www.bloomberg.com/news/articles/2021-07-14/facebook-fb-advertisers-impacted-by-apple-aapl-priva

[23] London Economics (2017), *Research and analysis to quantify the benefits arising from personal data rights under the GDPR, Report to the Department for Culture, Media & Sport,* https://www.oag.ca.gov/privacy/ccpa

below reproduces the results from a survey of data protection professionals on the likely benefits of the right to erasure:

Figure 1: Likely benefits of the right to erasure



Source: London Economics (2017) *Research and analysis to quantify the benefits arising from personal data rights under the GDPR*

The relevant exemptions would need to be investigated, including information that is of public benefit (e.g. regarding public figures and those who need to be held to account such as politicians), matters relating to public health, legal claims, national security or data for historical/scientific purposes, but ultimately a right to erasure would significantly protect individuals and balance the information and data asymmetry between them and large companies processing their data.

PLATFORM/ORGANISATIONAL ACCOUNTABILITY

Overall, responsibility and accountability for adequate privacy practices should be placed with the digital platforms/organisations. Digital platforms like Google and Meta generate

substantial profits from the collection and processing of individual personal information, and they therefore must be held to account for their business models.

Beyond the specific proposals and questions being investigated as part of this review, the overall theme of organisational accountability could appropriately capture the right concepts and frameworks with respect to privacy protections. These could include but should not be limited to:

- Privacy by design, building in privacy features and protections into the design and technical specifications of products and services, rather than retroactively trying to apply privacy features on an already finished product.
- Privacy by default, having the maximum level of privacy protections activated by default on products and services.
- Purpose limitations, making sure that data collection is restricted for the explicit and singular purpose to which it was consented to, and no secondary usage or extra data transfer is conducted
- Data separation, limiting the ability for companies to share user data between its different products and services (e.g. consenting to use Google Maps doesn't mean Google can use that location data to target users using Google Search)
- Data minimisation, only capturing the minimal amount of data

A STRONG, DIGITALLY SAVVY PRIVACY COMMISSION

It is not just the Privacy Act which needs to evolve for the Internet Age, its enforcing agencies must do so as well. The OAIC has done a commendable job of being the compliance regulator for the current Privacy Act. But with a new Privacy Act for the digital age, their capabilities also need to update accordingly.

Additional funding, resources and capabilities needs to be developed for the OAIC. While a dedicated Online Privacy Commission may not be suitable, the Review should be taken as an opportunity to provide the maximum amount of support to the OAIC in governing the new updates to the Act. This should include a multi-layered penalty system, an Ombudsman and/or Deputy Commissioner and a new statutory tort for privacy breaches. This would ensure there are effective penalties against large technology companies which often have more resources than regulatory bodies and attempt to lobby their way out of regulatory initiatives.[24]

[24] Feiner (2021), *Facebook spent more on lobbying than any other Big Tech company in 2020,* https://www.cnbc.com/2021/01/22/facebook-spent-more-on-lobbying-than-any-other-big-tech-company-in-2020.html

There are also some notable crossovers between the Privacy Act review and online privacy considerations as it relates to the disparate initiatives brought about by the Advertising Services Inquiry, the Disinformation Code, the Online Safety Act and the Consumer Data Right, and any new and relevant online policy initiatives.

There is therefore a need to coordinate between these regulatory initiatives, and the OAIC will need extra resources to do so.

Recommendations

The Australia Institute's Centre for Responsible Technology welcomes the opportunity to make a submission to this critical review and put forward the following recommendations:

- Ensure the appropriate level of technical information is captured as part of the updates to the relevant areas of 'personal information'. Looking at what Google captures alone will show extensive technical and inferred information, including location history, interest and hobbies and third party tracking
- Move away from 'notice and consent' models which have proven to be ineffectual, and place the regulatory burden on platforms rather than individuals, considering requirements such as:
    - **Purpose limitations,** making sure that data collection is restricted for the explicit and singular purpose to which it was consented to, and no secondary usage or extra data transfer is conducted
    - **Data separation,** limiting the ability for companies to share user data between its different products and services (e.g. consenting to use Google Maps doesn't mean Google can use that location data to target users using Google Search)
    - **Data minimisation,** only capturing the minimal amount of data
- Apply mandatory additional requirements for high-risk activities like a Data Protection Impact Assessment for large scale data collection and processing
- Create red lines and additional restrictions for sensitive data like biometrics and facial recognition, and where possible, ban this activity
- Have privacy by default features on all relevant activities
- Enable stronger user controls, including the right to object and the right to erasure
- Place responsibility on platforms, rather than individuals, by encouraging privacy by design and other privacy-friendly frameworks
- Evolve the Office of the Australian Information and Privacy Commissioner's (OAIC's) capabilities to meet these new demands, including additional penalties like multi-level privacy penalties, a new Ombudsman and/or Deputy Commissioner, and a new statutory tort for privacy breaches.

Conclusion

The Review of the Privacy Act is a most welcome and needed opportunity to address the privacy breaches being conducted by large technology companies through the vast collection and processing of Australians' personal information. Through proportionate, but progressive regulatory features the Privacy Act update could go towards protecting the privacy of Australians in the digital age. These updates should ensure the appropriate technical information is being captured, that we move beyond notice and consent models and towards more privacy by design frameworks, mandatory restrictions are placed for high-risk activities, and that the relevant enforcement capabilities are adequately resourced.