Australian Government

Attorney-General's Department

Enhancing online privacy and other measures

Early Assessment - Regulation Impact Statement

October 2021

Background

In March 2019, the government made a commitment to strengthen the *Privacy Act 1988* (Privacy Act) by introducing a binding code of practice for social media and other platforms that trade in personal information[1] online, and increasing penalties and enforcement measures.[2] This commitment was made to ensure that existing protections and penalties for misuse of Australians' personal information are updated and adequately reflect community beliefs and expectations. The exposure draft of the *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021* (the Online Privacy Bill) gives effect to these reforms.

The value of the government's commitment to strengthen privacy protections was reinforced by the Australian Competition and Consumer Commission's (ACCC) *Digital Platforms Inquiry* report (DPI report)[3]. The July 2019 report recommended the development of a privacy code for digital platforms, including social networks and an increase in penalties for breaches of the Privacy Act. Of particular concern was the asymmetrical relationship between consumers and digital platforms, which makes it difficult for users to be confident that their privacy is being protected.

The DPI report discussed the data-handling practices that underpin the business models of platforms such as Facebook, including data sharing with third-party companies – as in the Cambridge Analytica incident. In 2018, the UK data analytics firm was widely reported to have harvested the data of 50 million Facebook users without their consent in 2014, through an associated mobile app called 'thisisyourdigitallife'. The app had built psychological profiles on users and their Facebook friends. Cambridge Analytica sought to sell the data to political campaigns looking to target their messaging, at the time of major elections and referendums in 2016. Facebook later confirmed that as many as 87 million users could have been affected, including over 300,000 Australians. The Office of the Australian Information Commissioner (OAIC) alleges that the personal information of Australian Facebook users was disclosed for a purpose other than the purpose for which the information was collected for.

In its response to the DPI report, the government further committed to undertake a review of the Privacy Act[4] and to consult on options for implementing several recommendations specific to the Act, to better empower consumers, protect their data and best serve the Australian economy. The review commenced in October 2020[5]. Any amendments to the Privacy Act that follow will complement those in the Online Privacy Bill.

---

[1] Personal information is defined in the Privacy Act as information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether it is recorded in a material form or not.
[2] Joint Media Release, Tougher penalties to keep Australian safe online, 24 March 2019, 6577790.pdf;fileType=application/pdf (aph.gov.au)
[3] Digital platforms inquiry – final report, 26 July 2019, https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report
[4] Joint Media Release, Response to Digital Platforms Inquiry, 12 December 2019, https://parlinfo.aph.gov.au/parlInfo/download/media/pressrel/7079891/upload_binary/7079891.pdf;fileType=application%2Fpdf#search=%22media/pressrel/7079891%22
[5] Review of the Privacy Act 1988, https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988

As the government made a commitment to strengthen the Privacy Act by introducing these reforms, this Regulation Impact Statement (RIS) will only assess the one option to make the amendments in the Online Privacy Bill.

What is the problem to be solved?

Existing protections and penalties for the misuse of Australians' personal information fall short of community expectations, particularly in the context of social media platforms, and other online platforms that collect a high volume of personal information or trade in personal information.

The majority of Australians benefit from a wide range of valuable services provided to consumers for zero monetary cost, in exchange for their attention and user data. However, the DPI report found that several features of consumers' current relationship with digital platforms prevent consumers making informed choices. They include bargaining power imbalances, information asymmetries between digital platforms and consumers and consumers' inherent difficulties in accurately assessing the current and future costs of providing their user data.

The problem is exacerbated in the digital economy due to the large volume and scope of user data that is collected and used. This is central to the business model of most advertiser-funded platforms, such as social media organisations. The opportunities for social media and online platforms to collect and leverage user data is increasing due to the growing number of Australians who use and spend time on these platforms, and the number of services platforms now offer to users. For example, the DPI report found that Google provides over 60 different online services that provide Google with over 60 different sources of first-party user data that may be combined and associated with a single user account.

Private sector organisations subject to the Privacy Act must comply with the Australian Privacy Principles (APPs). The APPs are principles-based law that govern standards, rights and obligations regarding:

a) the collection, use and disclosure of personal information
b) an organisation or agency's governance and accountability
c) integrity and correction of personal information
d) the rights of individuals to access their personal information

However, the APPs do not effectively address the specific challenges posed by social media platforms, and other online platforms that collect a high volume of personal information or trade in personal information. Those challenges are outlined below.

Further, the existing protections and penalties for misuse of Australians' personal information under the Privacy Act are inadequate to ensure Australians are protected online and are trailing behind the protections and penalties that apply in other likeminded countries. To promote effective deterrence, it is essential for the Privacy Act to provide for meaningful sanctions for any conduct interfering with an individual's privacy.

Limitations of the Privacy Act in addressing the challenges posed by social media and online platforms

Consent

Consent is not currently required in all circumstances. Unless collecting sensitive information, a social media or online platform can collect personal information without consent, so long as the collection is reasonably necessary for its functions or activities. Much of the information that users share online, including photos and videos, as well as the

information that platforms collect about users, including location and other tracking data, is personal information that is not necessarily sensitive within the meaning of the Act. The Privacy Act also does not require organisations to ensure consent is kept current, nor does it dictate when it must be renewed.

While social media platforms may seek to obtain consent through terms of use agreements, individuals may have little recourse if they believe the consent they provided was not informed, voluntary or current, or they believe they did not have capacity to give consent.

Privacy policies and notices

Regardless of whether consent is required when collecting information, organisations must notify individuals when collecting information. This notice must include details of why they are collecting the information and what it will be used for. Further, organisations must demonstrate that they manage personal information openly and transparently, including by having a clearly expressed privacy policy. Information must also only be collected by lawful and fair means and from the individual themselves (unless it unreasonable or impracticable to do so).

However, the APPs do not set out how those privacy obligations are to be fulfilled. For example, the notification requirement does not prescribe how and when the individual must be made aware of the collection of their personal information (except that it must be done when practicable and where reasonable). Similarly, while the privacy policy must be clearly expressed and contain information about the purposes for handling personal information, there is no legislative requirement for the stated purposes to be detailed and unambiguous.

Further, the terms and conditions and privacy policies of these platforms may include information about their practices. However, such documents are often vague, lengthy, legalistic and difficult to comprehend. Compounding this information inadequacy is the imbalanced relationship between users and social media platforms. Social networks are often free to join, but users have limited bargaining power and are expected to exchange their data as a form of payment. They may agree to this exchange at a point in time to use the service. However there is little incentive to review the agreement on an ongoing basis and users may find it difficult to discern in advance what practices might occur in the future. There is also often no way of knowing whether and how an organisation will give effect to its promised protections.

Right to object

The APPs currently stipulate that an organisation must take reasonable steps to correct personal information held about an individual at the individual's request, and must destroy or de-identify personal information that is no longer required for a specific purpose under the APPs. However, there is no ability for an individual to request that an organisation does not use or disclose, or further use or disclose, an individual's personal information upon request from that individual. That is, the Privacy Act does not empower users to opt-out of certain data-handling practices.

Application of the Privacy Act to children and vulnerable groups

The privacy practices of online platforms can be detrimental to children and vulnerable persons, including engaging in harmful tracking, profiling, or targeted marketing. The privacy risks are exacerbated for children who use social media platforms, due to the ubiquitous nature of social media, the nature of the interactions that can occur via social media platforms, and the wide range and volume of personal information that social media platforms handle (location, gender, interests, hobbies, moods, mental health and relationship status).

The eSafety Commissioner's May 2018 'State of Play – Youth, Kids and Digital Dangers' Report[6] (the Report) found that children encounter a variety of negative experiences online, and nearly 6 in 10 respondents who reported a negative experience online in the 12 month assessment period identified emotional and/or psychological impacts as a result. The Report found that whilst a majority of children actively managed their online digital presence through the use of privacy settings, nearly half of children between the ages of 8 and 12 did not actively manage their online presence via social media. The Report also noted that parents and guardians have an important role to play in assessing a child's maturity, agency and ability to deal with the content and contacts that they may be exposed to while online.

To date, details about how privacy protections under the Privacy Act apply to children have been set out in guidance material from the Commissioner rather than in the Privacy Act itself. For example, the Commissioner's long-standing approach has been that entities should assess the capacity of individuals under the age of 18 on a case-by-case basis, and may presume that an individual over the age of 15 has the capacity to provide consent to collection, use or disclosure of personal information unless something suggests otherwise. The Commissioner's guidance material also mentions dealing with representatives of individuals who are otherwise not capable of making their own privacy decisions. However, the guidance material does not outline stronger and more robust privacy protections for the handling of personal information of children or vulnerable individuals.

Need for strengthened penalties and enforcement mechanisms

Penalties

Given the size of some entities collecting, using and disclosing information in the digital economy, which includes digital platforms operating in Australia, the ACCC recommended that the maximum penalties of the Privacy Act should be increased to mirror the recently increased penalties for breaches of the Australian Consumer Law.

The civil penalty for serious and/or repeated interferences with privacy is currently 2,000 penalty units (section 13G of the Privacy Act) — which, on the current penalty unit value, leads to a maximum civil penalty of $2.22 million for bodies corporate and $444,000 for an individual. These penalties fall short of community expectations, particularly if it is large multinational organisations being penalised.

The criminal penalty for an organisation refusing or failing to give information to the OAIC, or answer a question or produce a document or record when required to do so under the Privacy Act, is currently imprisonment for 12 months or 20 penalty units or both for an individual, or 100 penalty units for bodies corporate (section 66 of the Privacy Act). The OAIC has reported that investigations can be delayed due to the failure of parties to respond to requests for information issued under section 44 of the Privacy Act. A power to issue infringement notices for failing to comply with section 44 and similar provisions contained in the Act would encourage compliance, which would enable the OAIC to resolve matters more quickly.

[6] State of Play – Youth, Kids and Digital Dangers Report, May 2018, https://www.esafety.gov.au/sites/default/files/2019-10/State%20of%20Play%20-%20Youth%20kids%20and%20digital%20dangers.pdf

Determination

At the conclusion of an investigation of a complaint or an investigation commenced on the Commissioner's own initiative, the Commissioner can make a determination that:

a) the complaint is not substantiated, or the act or practice does not constitute an interference with privacy,
b) the complaint is substantiated, or the act or practice does constitute an interference with privacy, but that it would be inappropriate for any further action to be taken, or,
c) the complaint is substantiated, or the act or practice does constitute an interference with privacy, and the respondent must:
    i. take specific steps to prevent that conduct repeating or continuing,
    ii. perform an act or course of conduct to redress any loss or damage suffered by the complainant, and/or
    iii. pay compensation to a complainant.

The Commissioner does not currently have the express ability to require an entity to engage a qualified independent third party following a determination being made. Entities have agreed to follow this process when the Commissioner accepts an enforceable undertaking as an alternative to making a determination. The third party is able to review any relevant business practices or processes that contributed to the non-compliance, or to review the remediation of the non-compliance and provide the Commissioner with details about their findings. The value of this approach is that it provides a level of independent and expert assurance that non-compliance has been appropriately remediated.

Further, following a determination, the Commissioner does not have the power to publish, or require the organisation to publish, information regarding the investigation. This means that Australians are not always aware of emerging privacy issues, or notified when the Privacy Act is contravened by entities who hold their personal information.

Assessment of compliance

The Commissioner currently has the power to assess an entity's compliance with the Privacy Act, even in the absence of a breach of the Privacy Act or a complaint having been made. Although this is a valuable regulatory and educative tool to help identify emerging privacy issues, the existing power is limited as the Commissioner cannot directly assess an entity's compliance with the notifiable data breach scheme. Further, the Commissioner cannot compel entities to provide information that may be relevant to an assessment. This has meant that in practice, where an APP entity does not provide this information by consent, there may be obstacles to conducting assessments which require information that is not publicly available such as documents relating to APP entities internal governance arrangements, practices, procedures and systems.

Information sharing

The Commissioner is subject to a strict secrecy provision in the *Australian Information Commissioner Act 2010* that often prevents the Commissioner from sharing information obtained during the course of an investigation with other regulators or complaint bodies. In some cases, the Commissioner is unable to notify other regulators when it becomes apparent during a privacy investigation that an entity may have broken a law overseen by another regulator. The Commissioner is also limited in her ability to share information with Australians whose privacy has potentially been at risk of being compromised. This limits the ability for some Australians to take measures to protect their personal information.

Extraterritorial operation of the Privacy Act

Currently, foreign organisations must meet obligations under the Privacy Act if the entity has an Australian link. A foreign organisation will have an Australian link if the organisation or operator carries on business in Australia, and collects or holds personal information in Australia.

However, when a breach of the Privacy Act occurs, it may be difficult to establish that these foreign organisations collect or hold personal information from a source in Australia. This is because large multinational companies may collect personal information from Australian customers from an entity that is not incorporated in Australia, and transfer it to other entities overseas for processing and storage. When a breach of the Privacy Act occurs, it can be difficult to establish if the foreign organisation collected or held information 'in Australia' if there are multiple companies within the multinational group, in different overseas locations and performing different functions. Similarly, foreign organisations may collect and trade in data about Australians but do not collect Australians' information directly from Australia, and instead collect the information from a digital platform that does not have servers in Australia and may therefore not be considered 'in Australia'.

This has the potential to impede the Commissioner's ability to take effective regulatory action against overseas companies with adverse privacy impacts for Australians, and does not fulfil the original intention of the Act to capture foreign organisations who collect or hold personal information from people who are physically in Australia.

Who the problem affects and its potential magnitude

As social media plays a central role in the lives of many Australians, if the Privacy Act is not strengthened, the consequences would continue to be far-reaching. In 2020, the Consumer Policy Research Centre (CPRC) reported[7] that 58 per cent of Australians are daily users of Facebook and 40 per cent use other social media daily, including Instagram, Snapchat and Twitter. The eSafety Commissioner also recently reported[8] an increase in Australians' online activity as a result of COVID-19, including a significant increase in use of social media for entertainment (25 per cent of Australians reported using it a lot more). The survey found 43 per cent of Australians see communicating and interacting online with family and friends as essential to their day-to-day activities. Of particular concern, the eSafety Commissioner's May 2018 'State of Play – Youth, Kids and Digital Dangers' Report[9] highlighted the number of children who use social media platforms (83% of children surveyed used YouTube, 50% used Facebook, 47% used Instagram and 46% used Snapchat).

Despite the high use of social media and the internet more broadly, Australians are concerned about their privacy online. The OAIC's C*ommunity Attitudes to Privacy Survey 2020* (the 2020 OAIC survey)[10] found that 70 per cent of Australians consider the protection of their personal information to be a major concern in their life and 58 per cent identified digital services, including social media sites as presenting a privacy risk. Further, most

[7] CPRC 2020 Data and Technology Consumer Survey, 7 December 2020, https://cprc.org.au/publications/cprc-2020-data-and-technology-consumer-survey/
[8] Covid-19 impact on Australian adults' online activities and attitudes , June 2020, https://www.esafety.gov.au/sites/default/files/2020-06/Covid-19-impact-on-Australian-adults-online-report.pdf
[9] State of Play – Youth, Kids and Digital Dangers Report, May 2018, https://www.esafety.gov.au/sites/default/files/2019-10/State%20of%20Play%20-%20Youth%20kids%20and%20digital%20dangers.pdf
[10] Australian Community Attitudes to Privacy Survey 2020, September 2020, https://www.oaic.gov.au/assets/engage-with-us/research/acaps-2020/Australian-Community-Attitudes-to-Privacy-Survey-2020.pdf

Australians consider the social media industry the most untrustworthy in how they protect or use their personal information (70 per cent consider this industry untrustworthy), followed by search engines (55 per cent) and apps (54 per cent). Targeted advertising and collection and tracking of user data is also of concern; 58 per cent of respondents indicated discomfort with targeted advertising online and 62 per cent indicated discomfort over online platforms keeping databases of their online activity.

The OAIC's findings complement the 2020 CPRC survey, which found that only 6 per cent of Australians are comfortable with how their personal information is collected and shared online and only 12 per cent feel they had a clear understanding of how their information is being handled by companies, including social media platforms. Further, more than 60 per cent of Australians are uncomfortable with companies sharing their personal information with third parties for purposes other than delivering services they had signed up for. The overwhelming majority of Australians also find many data-handling practices of companies to be either very unfair or unfair, including the practice of selling or sharing their personal information to other companies.

The concerns Australians have about their privacy are being realised. The 2020 OAIC survey found the majority of Australians (59 per cent) had experienced problems with the handling of their personal information in the previous 12 months. Some reported having experienced the collection and intentional disclosure of their personal information by a business without their consent, when it was not required to deliver the service.

The 2020 OAIC survey indicated that, due to concerns about privacy, 57 per cent of Australians have deleted an app at some point and 46 per cent at least often provide false information to a company.

Why is government action needed?

Government action is needed to ensure the Privacy Act provides adequate protection for Australians using social media platforms, and other online platforms that collect a high volume of personal information or trade in personal information

In summary, the Privacy Act does not adequately address the following main concerns:

a) First, terms and conditions and privacy policies are often complex, vague and lengthy and can understate the extent of data-handling practices. Further, consent is often given at a point in time, typically when signing up for a service. Current approaches do not adequately account for changes in circumstance or in the nature of the service being offered.
b) Secondly, in many contexts informed consent is no longer seen by consumers as a meaningful concept. Even if they are uncomfortable with the content of a policy they may consent because that is the price of obtaining the service.
c) Thirdly, the penalties and enforcement mechanisms available to the Commissioner are inadequate and do not meet community expectations.

The concerns at a) to b) above are particularly relevant when an organisation is handling the personal information of children or vulnerable groups.

The Act does not address the above concerns because it does not:

a) impose specific requirements about how notice must be provided and consent obtained;
b) require online platforms to respond to requests from individuals to cease further use and disclosure of their personal information;
c) provide stricter rules in relation to personal information of children and other vulnerable groups;
d) contain penalties and enforcement mechanisms that enable the Commissioner to effectively resolve privacy complaints and investigations, and deter organisations from poor data-handling practices.

There is a strong community expectation that government will intervene in response to this problem. The 2020 OAIC survey found that 83 per cent of Australians would like the government to do more to protect their information privacy. The CPRC's 2020 report found that 79 per cent of Australians believe the government has a high level of responsibility to protect consumers against their information being used in ways that make them worse off. Specifically, 68 per cent believe the government is highly responsible for ensuring consumers have options to opt-out of various data collection, use and sharing practices.

The pervasive use of online platforms by Australians, including as a communication tool for schools, community groups, sports clubs and governmental bodies means that many Australians find that they must use digital platforms to participate in community life. This makes providing enhanced privacy protections all the more important.

What is the alternative to government action?

The alternative to government action is the maintenance of the current Privacy Act framework as it applies to social media platforms, and other online platforms that collect a high volume of personal information or trade in personal information. There are shortcomings with this approach as there is insufficient legislative authority for the Commissioner to take action that would fully address the above concerns.

Further, the current regulatory regime is not well placed to address large-scale or systemic misuse of personal information. Enforcement mechanisms require individuals to come forward with complaints and existing tools such as civil penalties and enforceable undertakings are not strong enough to act as a deterrent.

What are the objectives of government action?

The objectives of government action are to deal with the specific challenges to privacy posed by online platforms in a targeted way that does not impose a regulatory impact on other industry sectors. The Privacy Act must otherwise remain principles-based and technology neutral, to continue to encompass the different ways and purposes for handling personal information.

The challenges presented by online platforms are particularly important to address because of the vast amount and scope of personal information being collected online, and because there are likely very few Australians who are unaffected by their data-handling practices.

Overall, the objective of targeted regulation is to allow Australians to have more and better access to information about how online platforms collect, use and disclose their personal information, and the ability to request that these organisations cease any further use or disclosure of their information.

Does the government have the capacity to successfully intervene?

To address the particular privacy challenges posed by social media and online platforms it is necessary to adapt and expand upon the requirements under the APPs. This can be achieved through the development of a new Online Privacy Code (OP code) under the Privacy Act with the effect that a breach of the code is a breach of the Act. The process for developing a code is outlined below.

Code making process

The Commissioner can currently make two kinds of binding codes of practice under the Privacy Act (binding privacy codes):

a) an Australian Privacy Principle code (APP code) that sets out how one or more of the Privacy Act's APPs will apply to a particular entity or class of entities; or
b) a credit reporting code that sets out additional detail about how the Privacy Act's credit reporting provisions are to apply.

The Commissioner may ask an entity or an industry body to develop a legally binding code setting out how the Act applies to that entity or industry. If they decline, or produce a sub-standard code, the Commissioner can develop the code herself.

The codes may impose additional requirements to those imposed by the APPs or Privacy Act, but must not be contrary to or inconsistent with the APPs or Privacy Act. An entity bound by a registered code must not do an act, or engage in a practice, that breaches the code. A breach of a registered code is an interference with the privacy of an individual under the Act and subject to investigation by the Commissioner.

To fully address the challenges posed, it would be necessary for the Commissioner to make a third kind of binding privacy code to deal specifically with social media and online platforms. The existing APP code making power is limited as it is intended to build on existing APPs. As the APPs do not currently address specific concerns with social media and online platforms, this would limit the scope of an APP code to address these concerns.

The Privacy Act can be amended to require the Commissioner to make a third kind of binding privacy code, called the OP code. The OP code will set out how private sector organisations that provide social media platforms, or that collect a high volume of personal information or trade in personal information must (1) comply with the Privacy Act's APPs and (2) comply with additional obligations.

What policy options are being considered?

Only one option will be assessed, as the government made a commitment to strengthen the Privacy Act by introducing a binding online privacy code, and by strengthening enforcement measures and penalties.

Online Privacy code (OP code)

The Privacy Act will be amended to enable the introduction of a binding online privacy code (the OP code). The OP code will address the particular privacy challenges posed by social media and online platforms that collect a high volume of personal information or trade in personal information by adapting and expanding upon the existing requirements in the Privacy Act. The requirements in the OP code would operate in place of, or where applicable, in addition to, existing requirements in the Privacy Act. As with existing Privacy Act requirements, it is anticipated that the OP code would be framed in principles-based, technology neutral terms and would be supported by OAIC guidance material.

Who would the OP code apply to?

When determining which categories of online platforms should be subject to the OP code, consideration was given to the data practices of online platforms, bargaining power imbalances, and information asymmetries between the platforms and consumers. The Bill proposes that the OP code will apply to the following categories of private sector organisations that are already subject to the Privacy Act[11], who will be known as **OP organisations**:

a) **Social media platforms:**
   i. The OP code will apply to organisations that provide an electronic service that has the sole or primary purpose of enabling online social interaction between two or more end-users, allows interactions between end-users, and allows end-users to post material on the service.
   ii. An 'electronic service' will not include a 'broadcasting service' or 'datacasting service', a system that solely processes payments, or a system with the sole purpose of providing access to a 'payment system'.

b) **Data brokerage services:**
   i. The OP code will apply to organisations that provide a 'data brokerage service'. This is intended to capture organisations whose business model is based on trading in personal information collected online, or trading in information derived from such personal information, such as data derived from customer loyalty or frequent flyer schemes.
   ii. An organisation will provide a 'data brokerage service' if it collects personal information via an electronic service (other than a social media service), or collects personal information from another entity that collected the information via an electronic service; and collects the personal information for the sole or primary purpose of disclosing the personal information, or information derived from the personal information, in the course of providing a service.

c) **Large online platforms:**
   i. The OP code will apply to 'large online platforms'. This is intended to capture organisations who collect a high volume of personal information online.

[11] To be subject to the Privacy Act, a private sector organisation must: have annual turnover greater than $3 million, or engage in particular kinds of business activities — such as providing a health service, or trading in personal information without consent; and be based in Australia, or otherwise carry on business in Australia and collect or hold personal information in Australia (including via the internet).

ii. An organisation will be a large online platform if it collects personal information about an individual in the course of or in connection with providing access to information, goods or services (other than a data brokerage service) by use of an electronic service (other than a social media service); and has over 2,500,000 end-users in Australia in the past year, or if an organisation did not carry on business in the previous year then 2,500,000 end-users in the current year.
iii. An end-user is any individual who uses the electronic service – for instance it would include an individual who uses a search engine.
iv. An organisation would not be captured as a large online platform to the extent the organisation collects personal information about an individual in the course of or in connection with providing a customer loyalty scheme – for example if customers earn points or rewards for making purchases online.

Private sector organisations that are not already subject to the Privacy Act will not be subject to the OP code.

The three categories of OP organisations reflect that introducing stricter privacy regulation for social media platforms alone may not address privacy concerns arising from the broader online data sharing ecosystem. The large scale collection of and trading in end-users' personal information can escalate the harm arising from a privacy breach, and makes it difficult for users to be confident that their privacy is being protected

Feedback is sought on whether the scope of OP organisations strikes the right balance between the need to enhance privacy protections and the regulatory burden imposed on the proposed OP organisations. Feedback will be used to consider whether there is a need to revise the types of online platforms the OP code will apply to in order to ensure the code is appropriately targeted towards organisations with harmful online practices.

Requirements of the OP code

The Bill will set out the minimum requirements the OP code must include, as well as additional matters the code may address. Once developed, the OP code will set out these requirements in detail.

APP requirements

The OP code will be required to set out how the following APPs are to apply, or be complied with, by OP Organisations:

a) APP 1.4(c) about privacy policies: the OP code will require organisations to ensure that privacy policies clearly and simply explain the purposes for which they collect, hold, use and disclose personal information.
b) APP 5 about providing notice to individuals about collection of personal information: the OP code will require all notices to be clear and understandable, current, and provided in a timely manner. The OP code will also allow other notice requirements to be imposed in addition to those in APP 5.
c) APPs 3 and 6 about seeking consent for collection, use and disclosure of personal information: the OP code will require organisations to ensure that, when they seek consent from individuals, the consent is voluntary, informed, unambiguous, specific and current. For categories of personal information the Privacy Act treats as 'sensitive information' (such as health information), organisations will also need to seek renewed consent periodically or when circumstances change.

Requirement to cease using or disclosing personal information

The OP code will require organisations to take such steps (if any) as are reasonable in the circumstances to not use or disclose, or to not further use or disclose, an individual's personal information upon request from that individual. This requirement is not intended to amount to a 'right to erasure' of the personal information, and will not prevent 'secondary' uses and disclosures of personal information that are currently permitted under the Privacy Act. Specifically, the new requirement will not prevent uses or disclosures that are:

a) authorised or required by or under another Commonwealth, State or Territory law or court or tribunal order;
b) are reasonably necessary to assist a law enforcement body undertake an enforcement-related activity;
c) or occur during a 'permitted general situation' or a 'permitted health situation', for example, in response to a serious threat to individual or public health or safety.

Organisations will be required to respond to a request in a reasonable time period. If the organisation cannot comply with the request, it will need to provide the individual with a written notice providing reasons and the available avenues of complaint (including the availability of complaints to the Commissioner). Organisations will only be able to impose reasonable charges for responding to the request. Charges could not be imposed to the act of making the request or if the organisation is unable to comply with the request. These procedural requirements are modelled on APP 12 (access to personal information).

Requirements relating to children and vulnerable persons

The OP code will require OP organisations to comply with the following protections in relation to children or other groups of people not capable of making their own privacy decisions:

a) For all OP organisations:
    i. The OP code will need to set out how all the above requirements will apply in relation to children or other groups of people not capable of making their own privacy decisions, including imposing more specific obligations if necessary.
    ii. In addition, the OP code will be required to include specific provisions about how consent for the collection, use or disclosure of personal information should be provided either by those individuals, or parents, guardians or representatives of those individuals.
b) For social media platforms:
    i. The potential risks social media platforms pose to children are higher than those posed by data brokers or large online platforms due to the number of children who use social media services, the nature of the interactions that can occur via social media platforms, and the wide range and volume of personal information that social media platforms handle. To address these risks, the OP code will have stricter requirements for how social media platforms handle children's personal information (with children being defined as an individual who has not reached 18 years of age).
    ii. In addition to the above requirements, the OP code will require social media platforms to:
        a. Take all reasonable steps to verify the age of individuals who use the social media service; and
        b. Ensure the collection, use or disclosure of a child's personal information is fair and reasonable in the circumstances, with the best interests of the child being the primary consideration when determining what is fair and reasonable; and

c. Obtain parental or guardian consent before collecting, using or disclosing the personal information of a child who is under the age of 16, and take all reasonable steps to verify the consent. In the event that a social media service becomes aware that an individual was under the age of 16 (for instance if they had new information to suggest an individual previously believed to be over the age of 16 was in fact not), the social media service must obtain verifiable parental or guardian consent as soon as practicable.

iii. Factors relevant to whether the collection, use or disclosure of a child's personal information is fair and reasonable or what reasonable steps would need to be taken for verification may be outlined in the OP code (and/or the Commissioner's guidance material). This could include, for example, requiring certain acts and practices (such as default privacy settings), or limiting certain acts and practices (including online tracking, behavioural monitoring and profiling of children, disclosure of a child's personal information to a third party, and the sale of a child's personal information).

Optional requirements

The Bill will specify that the OP code may set out the following requirements, if the Commissioner or OP code developer wish to use them, or expand or clarify the obligations or procedures within the OP code. These requirements are optional, allowing the OP code to be flexible and responsive:

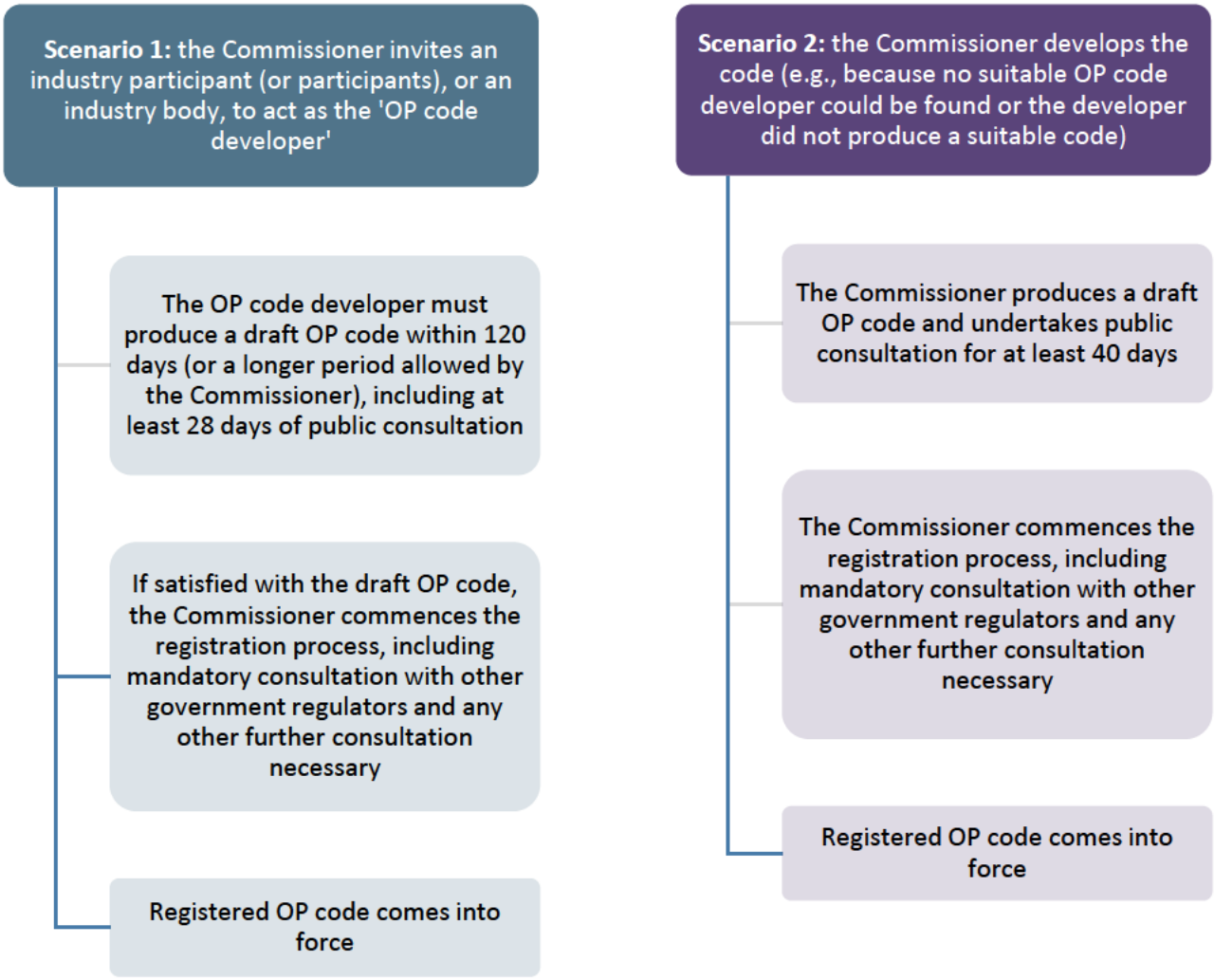
a) set out how one or more of the APPs that are not otherwise covered are to be applied or complied with;
b) impose additional (but not contrary or inconsistent) requirements to the APPs;
c) provide mechanisms to deal with the internal handling of complaints;
d) provide for the reporting of complaints to the Commissioner;
e) provide for reporting about the number of end-users in Australia for large online platforms; and
f) any other relevant matter.

<u>Code making process</u>

Industry will have the first opportunity to act as the 'OP code developer' and draft the OP code. The Commissioner will invite an organisation or a group of such organisations that would be bound by the OP code, or one or more industry bodies or associations representing such organisations, to act as the OP code developer. The Commissioner will consider whether the potential code developer has the capacity to develop a code including whether they have the resources and expertise, and is generally representative of the social media and online platform industry. The OP code developer would be required to undertake public consultation on the draft OP code for at least 28 days before submitting the finalised code to the Commissioner for approval.

If the Commissioner cannot identify an appropriate OP code developer, or the OP code developer does not comply with the Commissioner's request to develop the code, or the Commissioner is not satisfied with an OP code developed by the OP code developer, the Commissioner will have the discretion to develop the OP code herself. The Commissioner would be required to undertake public consultation on the draft OP code for at least 40 days. The longer timeframe compared to an industry-developed OP code reflects the fact that industry may need more time to consider a Commissioner-developed OP code than one prepared by an industry OP code developer.

The diagram below sets out two alternative scenarios for how the OP code will be developed:



Strengthen penalties and enforcement mechanisms

In addition to the OP code, the Bill will strengthen penalties and enforcement mechanisms for all entities regulated by the Privacy Act (not just OP organisations). The majority of the amendments will only have a regulatory impact on organisations that do not comply with the Privacy Act. The exception to this is the amendment to enhance the Commissioner's capacity to conduct assessments on organisations, which may occur without a breach of the Privacy Act occurring or a complaint being made.

<u>Increasing the maximum civil penalty for serious and/or repeated interference with privacy of an individual</u>

For a natural person, the Bill increases the maximum civil penalty for serious and/or repeated interferences with privacy to 2,400 penalty units ($532,800 on current penalty unit values). For a body corporate, the maximum penalty will increase to an amount not exceeding the greater of:

a) $10 million;

b) three times the value of the benefit obtained by the body corporate from the conduct constituting the serious and/or repeated interference with privacy; or
c) if the benefit cannot be determined then 10% of their annual domestic turnover.

These changes are consistent with maximum penalties under the Australian Consumer Law.

Creating a new infringement notice for failing to give information, or to provide a document or record when required as part of the Commissioner's investigation

Currently, section 66 of the Privacy Act creates a criminal offence where a person refuses to or fails to give information, or answer a question or produce a document or record when required to do so under the Act.

To enable the OAIC to resolve matters more efficiently, an infringement notice provision will be created to supplement a new civil penalty provision which will provide an alternative to prosecution for an offence and early resolution to potential litigation of a civil matter. An infringement notice may be issued by the Commissioner, or a member of staff of the Commissioner who is equivalent to a Senior Executive Service employee, where a person fails to comply with the requirement to give information, or provide a document or record when required under the Privacy Act. The penalty for the new civil penalty provision will be 60 penalty units for individuals, and 300 penalty units for bodies corporate—which, on the current penalty unit value, would result in a maximum civil penalty of $13,320 for individuals and $66,600 for bodies corporate.

A separate criminal offence will be created for where a body corporate engages in conduct which constitutes a system of conduct or pattern of behaviour. This would enable the OAIC to refer matters to the Commonwealth Director of Public Prosecutions for more serious, systemic conduct. The maximum penalty will be increased to 300 penalty units for bodies corporate— which, on the current penalty unit value, would result in a maximum civil penalty of $66,600 for bodies corporate.

Expanding the types of declarations that the Commissioner can make in a determination at the conclusion of an investigation.

To complement the Commissioner's existing power to make a determination that a respondent must take specified steps to ensure conduct constituting an interference with privacy is not repeated or continued, it will be clarified that the Commissioner could also require the respondent to engage, in consultation with the Commissioner, an independent and suitably qualified adviser to assist this process. The respondent would need to cooperate with the adviser and provide information on the following:

a) the acts or practices engaged in by the respondent that were the subject of the complaint; and
b) the steps (if any) taken by the respondent to ensure that the conduct referred to in the determination is not repeated or continued; and
c) any other matter specified in the declaration that is relevant to those acts or practices, or that complaint.

The adviser will then provide a copy of the review to the Commissioner. These provisions formalise the legal basis for a practice that the Commissioner has successfully used in multiple determinations in recent history.

These types of orders would mostly be made in large scale and complex matters. This would provide accountability and confidence for the Australian community while also serving as a deterrence for larger entities to ensure they comply with the Privacy Act. The cost of complying with these types of orders will vary depending on the type of determination, the relevant entity in question, and the adviser. The costs of such an order would be considered

by the Commissioner when making a determination to ensure that these expenses are proportionate in the circumstances.

Estimated costs and impacts for entities engaging with an adviser are outlined below:

a) The costs of an adviser will depend on the scope of the investigation and the type of investigator (which may be a lawyer, a consultant or a cyber security/IT specialist). It is estimated that an adviser may charge between $100-$300 per hour for a junior staff member, and between $300-800 per hour for a senior staff member.
b) The number of hours required to complete the review will also depend on the scope and number of the issues, and the size of the entity. For minor interferences with privacy, a review is likely to be undertaken in approximately 10 hours whereas a complex review for a large entity may take up to 200 hours.
c) The number of hours that an entity would be required to cooperate would depend on the involvement of the adviser and the complexity of the review, but it is estimated that for complex reviews an entity would be required to dedicate resources to assist the adviser with the review.

Additionally, a new determination power would be made available to the Commissioner to require the respondent to prepare a statement about the conduct that led to the interference of privacy. If the Commissioner chooses to use this power, the respondent would need to prepare a statement within 14 days after receiving the determination that identifies them, a description of the conduct they engaged in that constitutes an interference with privacy, steps taken by the respondent to ensure the conduct isn't repeated, and any other information required by the Commissioner's determination to be included in the statement. The Commissioner would be able to require the respondent to publish the statement and/or provide a copy to the complainant.

Estimated costs and impacts for entities preparing a statement would be minimal. This is because the Commissioner's determination would outline a majority of the required information, and the OAIC may also be able to assist and provide guidance on what steps may be required to ensure a breach is not repeated, particularly for less sophisticated entities. Further, publication in many cases is likely to be on the entity's website. While entities may choose to engage with lawyers to assist in the drafting of the statement, it is not required.

Enhancing the Commissioner's capacity to conduct assessments

The Bill enables the Commissioner to conduct an assessment of entities' compliance with the Privacy Act's Notifiable Data Breaches scheme[12], which commenced in February 2018. This would extend the Commissioner's existing power to conduct assessments of regulated entities to ensure they are handling information in accordance with legislation. The Privacy Act notes that the Commissioner may conduct an assessment in a manner the Commissioner considers appropriate.

A new information-gathering power for the purposes of conducting an assessment, of any kind, would also be available. The Commissioner would be able to issue a notice to produce information or a document relevant to the assessment, subject to the following safeguards:

a) a notice can only be issued to the entity or file number recipient subject to the assessment;

[12] Under the Notifiable Data Breaches scheme any organisation or agency the Privacy Act covers must notify affected individuals and the OAIC when a data breach is likely to result in serious harm to an individual whose personal information is involved.

b) the Commissioner must be satisfied that issuing a notice is reasonable in the circumstances, having regard to the public interest, the impact on the entity or file number recipient to comply with the notice, and any other matters the Commissioner considers relevant;
c) a law enforcement body is not required to comply with the notice if it would be likely to prejudice one or more of its enforcement related activities;

Failure to lawfully comply with the assessment notice would be subject to the new infringement notice power or criminal penalty for a failure to give information to the Commissioner when required. Estimated costs and impacts for entities complying with an assessment notice would be minimal.

Improving the Commissioner's information-sharing arrangements with relevant enforcement bodies and complaint bodies

The Commissioner would have the ability to share information or documents with the following:

a) a law enforcement body;
b) an alternative complaint body; and
c) State, Territory or foreign privacy regulators.

The ability to share information would not only be available to the Commissioner in the context of transferring a complaint to another body, but for the purpose of the Commissioner or receiving authority exercising any of their respective functions and powers.

The Commissioner's ability to share information and documents would be subject to the following limitations:

a) information sharing must be for the purposes of the Commissioner's, or the receiving authority's, exercise of powers or performance of functions and duties;
b) the information or documents must have been acquired by the Commissioner in the course of exercising powers, or performing functions or duties, under the Privacy Act;
c) the Commissioner must be satisfied on reasonable grounds that the receiving authority has satisfactory arrangements for maintaining the security of the information or documents; and
d) where the Commissioner has obtained information or documents from an Australian Government agency, the Commissioner would only be able to share those documents with an Australian Government law enforcement agency or alternative complaint body.

Disclosure of information

To ensure Australians are informed about privacy issues and can take measures to protect their personal information, the Commissioner would have the power to disclose information relating to privacy and information on the OAIC's website.

The Commissioner will have the ability to confirm whether the OAIC has received notice of an eligible data breach, and disclose information regarding assessment reports, section 52 determinations and enforceable undertakings without needing to meet a public interest test. It would be within the reasonable expectations of all parties and the community that such decisions would be disclosed.

For all other disclosures, for example information about ongoing investigations, the Commissioner must be satisfied on reasonable grounds that it is in the public interest to

disclose the information. To determine whether the disclosure is in the public interest, specific regard must be given to:

a) the rights, freedoms and legitimate interests of any person including the complainant or respondent
b) whether the disclosure could prejudice an investigation which is underway
c) whether the publication will or is likely to disclose the personal information of any person
d) whether the publication will or is likely to disclose confidential commercial information

Expand the extra-territorial application of the Privacy Act

The extra-territorial application of the Privacy Act would be clarified by removing the requirement that an organisation has to collect or hold personal information from sources inside of Australia. This would mean that foreign organisations who carry on a business in Australia must meet the obligations under the Privacy Act, even if they do not collect or hold Australians' information directly from a source in Australia. For example, an organisation that collects personal information of Australians from a digital platform that does not have servers in Australia will more clearly be subject to the Privacy Act.

What is the likely net benefit of each option?

Who would be affected

Businesses

OP Organisations would be subject to the new OP code, as discussed above.

All businesses subject to the Privacy Act, and not just OP organisations, would face increased regulatory impacts if they were required to cooperate with an assessment by the Commissioner. This may require the business to cooperate with the assessment and produce information or a document relevant to the assessment (subject to appropriate safeguards on the requirement to cooperate).

All businesses subject to the Privacy Act may face increased regulatory impacts in the following circumstances of non-compliance:

a) If a business breaches the Privacy Act by engaging in practices that are found to be a serious and/or repeated interference with privacy thereby attracting the increased Privacy Act penalties;
b) If a business breaches the Privacy Act by refusing or failing to give information or answer a question or produce a document or record when required to do so;
c) If the Commissioner requires as part of the determination process for the business to engage in an independent and suitably qualified adviser, or prepare a statement about the conduct that led to the interference with privacy.

All businesses may also benefit from improved OAIC education material and programs, reflecting the Commissioner's increased ability to understand emerging systemic privacy issues.

Individuals

Individuals would benefit from the creation and enforcement of the OP code, and in particular children. This will provide confidence to the public that the OAIC is able to safeguard their privacy rights and act as a deterrent against social media and online platforms utilising personal information in a manner inconsistent with the expectations laid out in Australia's privacy legislation.

In particular, individuals would have the ability to rely on the OP code to request that online platforms cease further use or disclosure of their personal information, as well as increased protections for personal information about children and vulnerable groups. There would be minor administrative burden for individuals, as they would be required to submit their own request and pay a reasonable charge (as outlined above).

Individuals will benefit from organisations facing increased penalties for breaches of the Privacy Act, and the Commissioner having stronger enforcement mechanisms. The reforms would improve the Commissioner's complaint clearance rates, encourage entities to engage in conciliation or remediation processes when they have contravened the Privacy Act, and send a message about the government's intention to introduce a stronger privacy enforcement framework.

Expanding the Commissioner's assessment powers will also help the Commissioner identify emerging systemic privacy issues before non-compliance has occurred, and allows the Commissioner to appropriately target educational materials and programs in response.

Costs

Costs for the chosen option, and key assumptions about the process of creating the code are outlined below. An hourly default rate of $73.05 has been used.

a) Based on development of previous Privacy Act codes, the one-off cost for an OP code developer to develop the OP code under the new Privacy Act code-making power is assumed to be **$882,078.75.**
    i. It is assumed that **two** industry bodies would participate in the code-making process. The cost above reflects two industry bodies participating.
b) It is assumed that the OP code would apply to **500 organisations** (approximately 150 social media platforms, 85 data brokers, and 265 large online platforms).
c) Initial code implementation costs are assumed to be **$2,191,500**. It is assumed that the implementation costs would include 60 hours of staff time incurred by each of the 500 organisations that will be subject to the OP code.
d) Social media platforms would have additional implementation costs due to the stricter requirements for handling personal information.
    i. Additional implementation costs for social media platforms to set up processes for requirements (including verification processes) is assumed to be **$876,600.** It is assumed that the implementations costs would include 80 hours of staff time incurred by each of the 150 social media platforms that will be subject to the OP code.
    ii. It is assumed that social media platforms will need to meet age and consent verification for the majority of its existing users to continue to provide electronic services to these individuals, and continue to collect, use or disclose the personal information of children aged under 16.
    iii. It is assumed that social media services will develop automatic verification processes for age and consent verification, but that the verification process would still require an average of 5 minutes of staff time per verification, totalling $6.09 per verification.
    iv. Additional implementation costs for social media platforms to verify the age of users, and verify the necessary parental/guardian consent is estimated to be **$526,203,500.**
        i. It is assumed that approximately 20,800,000 users will need to have their age verified. It is assumed that each of these users have 4 social media accounts.
        ii. It is assumed that approximately 810,000 children aged under 16 will need to have parental/guardian consent verified. It is assumed that each of these children have 4 social media accounts.
e) Business as usual compliance costs for the OP code for all OP organisations are assumed to be **$5,697,900 per annum.** It is assumed that business as usual compliance costs would include 3 hours of additional staff time per week incurred by each of the 500 organisations that will be subject to the OP code.
f) Social media platforms would have additional business as usual compliance costs due to the stricter requirements for handling children's personal information.
    i. Business as usual compliance costs for social media platforms is assumed to be $**1,139,580 per annum.** It is assumed that business as usual compliance costs would include 2 hours of additional staff time per week incurred by each of the 150 social media platforms that will be subject to the OP code.

ii. Business as usual compliance costs for social media platforms to verify the age of users, and verify the necessary parental/guardian consent for new users is assumed to be **$1,095,750 per annum.** It is assumed that approximately 22,500 individuals will sign up for 4 social media accounts each year. It is assumed that these individuals will likely be under the age of 16 and require both age verification, and need to have parent/guardian consent verified.

g) Increased cost of complying with Commissioner assessments, based on past assessment numbers and patterns, is assumed to be **$10,227 per annum**. This will apply to all entities regulated by the Privacy Act, and not just organisation subject to the OP code.

h) This results in a total one-off code development and implementation costs of **$530,153,678.75.** After implementation, the ongoing regulatory costs would be **$7,943,457 per annum** for organisations or **$79,434,570 over 10 years**.

Regulatory burden estimate (RBE) table per OP organisation

Average annual regulatory costs		
Change in costs ($ million)	Business	Total change in cost
Social media services (for total of 150 organisations)	$56,744,917.36*	$56,744,917.36*
Data brokerage services (for total of 85 organisations)	$1,020,893,84*	$1,020,893,84*
Large online platforms (for total of 265 organisations)	$3,182,786.67*	$3,182,786.67*
All entities regulated by the Privacy Act	$10,227.00	$10,227.00
TOTAL	$60,958,824.88	

*Includes code development costs and implementation costs averaged over a 10 year period, and business as usual annual costs.

Net benefits

The net benefits of this option are:

a) it addresses the specific privacy challenges posed by social media and online platforms. An OP code would enhance privacy protection in the online sphere without unduly impeding innovation within the digital economy, and give users more

control over their personal information. In particular, the OP code will address the specific privacy risks posed to children online.

b) it bolsters the OAIC's ability to regulate, and have effective oversight of businesses subject to the Privacy Act. This is critical to creating trust and improving public confidence that the OAIC is able to protect Australians' privacy in an efficient, just and effective manner.

Who will be consulted about these options?

In the development of the draft Online Privacy Bill, the Attorney-General's Department consulted with the following departments:

a) Department of the Treasury
b) Department of Home Affairs
c) Department of Industry, Science, Energy and Resources
d) Department of Infrastructure, Transport, Regional Development and Communications
e) Department of the Prime Minister and Cabinet
f) Office of the eSafety Commissioner
g) Office of the Australian Information Commissioner

Feedback was used to ensure the Online Privacy Bill aligned with related legislation and initiatives where appropriate (including the *Enhancing Online Safety Act 2015* and Consumer Data Right), provided for appropriate information sharing mechanisms between regulators, and ensured that the regulatory burden and scope of regulatory requirements was appropriately balanced with the need to enhance privacy protections and enhance enforcement mechanisms.

The draft Online Privacy Bill, alongside this consultation RIS and an explanatory paper, have been released for public consultation. Submissions close **6 December 2021.** This provides an opportunity for members of the public, businesses, non-profit organisations and public sector agencies to make submissions.

The Attorney General's Department will publish submissions received, unless submitters have asked for the submission to remain confidential or the department considers (for any reason) that it should not be made public.

Submissions and feedback received from the consultation process will be used to shape the development of the draft Online Privacy Bill before the legislation is settled for introduction in Parliament. The consultation process will also provide stakeholders an opportunity to provide feedback on the RIS, including on regulation impact assumptions and opportunities to reduce regulatory costs.

What is the best option from those considered?

Although the option considered will result in increased estimated regulatory costs, it is expected to provide a net benefit. The option would address all of the specific privacy challenges posed by online platforms discussed in this RIS, in terms of providing Australians:

a) greater transparency about how social media platforms, and other online platforms that collect a high volume of personal information or trade in personal information collect, use and disclose their personal information;
b) the ability to request platforms cease further use and disclosure of their personal information; and

c) greater assurances about how platforms handle personal information about children and other vulnerable groups.

Further, the option includes consideration of recommendations from the DPI report, which recommended the development of a privacy code for digital platforms, including social networks and an increase in penalties for breaches of the Privacy Act. The government undertook a 12-week consultation process when developing its response to the DPI report, including on the privacy-related recommendations.

The option would also bring Australia closer into line with the privacy frameworks in other jurisdictions, for example, the EU's General Data Protection Regulations (GDPR). The GDPR introduced a revised, narrower definition of consent, which must be a freely given, specific, informed and unambiguous indication of the data subject's wishes; introduced a right to erasure; and introduced stricter rules about how online services should seek consent when collecting personal information of a child.

How will you implement and evaluate your chosen option?

Implementation

The chosen option will be implemented through legislative changes to the Privacy Act, and consequential amendments to the *Australian Information Commissioner Act 2010, Australian Human Rights Commission Act 1986,* and the *Competition and Consumer Act 2010.*

If the Online Privacy Bill is passed and receives Royal Assent, the Commissioner or a chosen industry participant is able to start developing the OP code in accordance with the requirements outlined in the Online Privacy Bill. The OP code must be developed and registered within 12 months of the Online Privacy Bill passing and receiving Royal Assent.

Evaluation

The Attorney General's Department will evaluate the operation and impact of the proposed reforms on an ongoing basis. This evaluation will be informed by the OAIC's monitoring of the OP code's performance and its privacy assessments of organisations. The OAIC has an analysis and reporting function and produces quarterly and annual reports. Relevant statistics will include the number and nature of complaints made to the Commissioner regarding any matters in the OP code, including where an online platform refuses an individual's request to cease further use and disclosure of their personal information. If the Code requires platforms to report internal complaints to the Commissioner, those statistics may also be available.

To review the effectiveness of the reforms, the department will also closely monitor the feedback it receives from relevant stakeholders. This will complement any feedback received by the OAIC, including through its established stakeholder engagement program, as well as the feedback it receives through its existing online enquiry form and hotline. Additionally, the OAIC will receive feedback from organisations that are bound by the OP code, stakeholders that engage in the code-making consultation process, and as part of the Commissioner's expanded assessment powers.