October 2021

Explanatory paper

Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021

Contents

Introduction

The growth of social media and online platforms has posed new challenges to the protection of individuals' privacy in the digital age. Although over 17 million Australians use social media, the *Privacy Act 1988* (Privacy Act) does not currently provide specific protections against the misuse of Australians' personal information by social media and other online platforms.

At present, private sector organisations subject to the Privacy Act must comply with the Act's Australian Privacy Principles (APPs). However to address the particular privacy challenges posed by social media and online platforms in complying with the APPs in the online space, it is necessary to provide greater detail and adapt some of the APPs to this context.

In response to the Facebook/Cambridge Analytica data harvesting incident in March 2018, the Government committed to strengthening privacy protections by introducing a binding code of practice for social media and other online platforms that trade in personal information, and by enhancing enforcement mechanisms and penalties provisions under the Privacy Act. The Australian Competition and Consumer Commission's (ACCC) *Digital Platforms* July 2019 report reinforced the value of the Government's earlier commitment by recommending the development of a privacy code for digital platforms and increasing penalties for breach of the Privacy Act. The report examined the impact of digital platforms on competition in the media and advertising service markets and recommended strengthening protections in the Privacy Act and the development of a digital platforms code of practice.

These measures will be implemented through amendments in the *Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021* (Bill). The Bill will enhance the protection of personal information by enabling the introduction of an Online Privacy code (OP code), and enhancing penalties and enforcement measures. This paper contains a brief summary of the Bill. Further information about the general policy problem the Bill addresses, why the Bill is the preferred solution to that problem, and the expected regulatory impacts are outlined in the Regulation Impact Statement (RIS).

The Government seeks feedback on the Bill, particularly regarding the scope of organisations who will be required to comply with the OP code and the expected regulatory impacts of reforms on individuals and businesses. The goal of the Bill is to enhance privacy protections, particularly in the online sphere, without unduly impeding innovation within the digital economy. Submissions and feedback received from the consultation process will be used to shape the development of the Bill before the legislation is settled for introduction in Parliament.

The Bill addresses the particular and pressing privacy challenges posed by social media and online platforms. A broader review of the Privacy Act is being conducted in parallel[1], which will build on the outcomes of the Bill and ensure privacy settings empower consumers, protect their data and best serve the whole of the Australian economy.

[1] Attorney-General's Department, *Review of the Privacy Act 1988*

Have your say

The Government invites submissions on the exposure draft of the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 and the RIS by **6 December 2021**. The Government will consider all submissions received in the process of preparing a final draft Bill to present before Parliament.

If you have any questions, please contact OnlinePrivacyBill@ag.gov.au

We may publish your submission, unless you request for it to remain confidential, or if we consider (for any reason) that it should not be made public. We may redact parts of published submissions, as appropriate. Refer to our privacy policy to find out more.[2]

[2] Attorney-General's Department, *Privacy Policy*

Part A: Online Privacy code provisions — Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021

The development of a new OP code will address the particular privacy challenges posed by social media and other online platforms that collect a high volume of personal information or trade in personal information by adapting and expanding upon the requirements under the APPs.

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

- 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
- a credit reporting (CR) code that sets out additional detail about how the Privacy Act's credit reporting provisions are to apply.

The Bill will require a third kind of binding privacy code to be in place, called the OP code. The OP code will set out how certain private sector organisations must (1) comply with the Privacy Act's APPs and (2) comply with additional obligations.

The process for making the OP code will be similar to the process for the two existing Privacy Act codes, including giving industry the first chance to develop the OP code and requiring public consultation.

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.

Who will need to comply with the OP code?

It is proposed that the OP code will apply to the following categories of private sector organisation that are already subject to the Privacy Act[3], referred to as **OP organisations**:

1. Organisations that provide social media services; and
2. Organisations that provide data brokerage services; and
3. Large online platforms.

These organisations will need to meet the requirements of the OP code, as well as the ordinary provisions of the Privacy Act. Further detail about the OP organisations is set out in the table below. Further information regarding the regulatory burden imposed on the proposed OP organisations can be found in the RIS.

[3] 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).

For the purposes of the OP code, the definition of 'electronic service' will capture a broad range of existing and future technologies, including hardware, software, websites, mobile applications, hosting services, peer-to-peer sharing platforms, instant messaging, email, SMS and MMS, chat services, and online gaming.

An 'electronic service' will not include:

- a 'broadcasting service' or 'datacasting service' (as defined in the *Broadcasting Services Act 1992*);
- a system that solely processes payments;
- a system with the sole purpose of providing access to a 'payment system' (as defined in the *Payment Systems Regulation Act 1998).*

Table 1: Categories of private sector organisations subject to the OP code

Category of organisation	Description
Social media services	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, and allows interactions between end-users, and allows end-users to post material on the service. Examples of social media services include: • Social networking platforms such as Facebook • Dating applications such as Bumble • Online content services such as Only Fans • Online blogging or forum sites such as Reddit • Gaming platforms that operate in a model which enables end-users to interact with other end-users, such as multiplayer online games with chat functionalities • Online messaging and videoconferencing platforms such as WhatsApp and Zoom This definition is not intended to capture organisations that enable online communication/interactions/content sharing as an additional feature – for example, business interactions with customers such as online feedback facilities.
Data brokerage services	The OP code will apply to organisations that provide a 'data brokerage service'. An organisation will provide a 'data brokerage service' if it: • collects personal information from an individual 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 (including a social media 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 or in connection with providing a service. This is intended to capture organisations whose business model is based on trading in personal information collected online, or information derived from such personal information, such as data derived from rewards or loyalty programs. Organisations that collect personal information and disclose it for a secondary purpose will not be captured as a data broker. For example, a charity which collected personal information from donors and then later disclosed this information to a marketing agency to promote a fundraising campaign to previous donators would not be captured. Examples of data brokerage services include Quantium, Acxiom, Experian and Nielsen Corporation.
Large online platforms	The OP code will apply to 'large online platforms'. 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, 2,500,000 end-users in the current year. An end-user is any individual who uses the electronic service – for instance it would include an individual who uses a search engine. This is intended to capture organisations who collect a high volume of personal information online. Examples of large online platforms include major global technology companies (such as Apple, Google and Amazon) and media sharing platforms (such as Spotify). 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. Customer loyalty schemes are being considered as part of the Privacy Act Review.
Other organisations, or classes of organisations, named in a legislative	A legislative instrument power to apply the OP code to other organisations, or classes of organisations, will provide flexibility to respond to the fast-moving online environment if necessary.

instrument made by the Attorney-General	The Attorney-General would also have the power to make a legislative instrument excluding organisations, or classes of organisations, from the OP code. Before making any of the above legislative instruments, the Attorney-General would need to be satisfied that the instrument would be in the public interest, and consult the Information Commissioner. Any legislative instruments would also be subject to normal Parliamentary review and disallowance processes

Exclusions from the OP code

The OP code will not apply to particular kinds of acts and practices done that are exempt under the Privacy Act. These exclusions will match the existing exclusions that apply to APP codes and the general provisions of the Privacy Act itself. In particular, an organisation will not breach the OP code only because of an act or practice done or engaged in:

- under contract with an Australian Government agency (although the Privacy Act would still require agencies subject to the Act to include appropriate privacy protections in the contract); or
- outside of Australia, in compliance with an applicable foreign law.

The OP code will also not apply to Australian Government agencies. This is because the OP code deals with particular kinds of commercial activities that agencies are unlikely to undertake. Agencies subject to the Privacy Act are, however, already subject to heightened privacy obligations under an APP code called the *Privacy (Australian Government Agencies — Governance) APP Code 2017*.

What will be the requirements of the OP code?

The OP code will need to address how certain existing APPs apply to OP organisations, how new obligations will apply to OP organisations, and how both existing and new obligations will apply in relation to children and vulnerable groups. The OP code will also be able to deal with other specified matters.

Existing Australian Privacy Principles that the OP code must address

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

- **APP 1.4(c) about privacy policies**: the OP code will require entities to ensure that privacy policies clearly and simply explain the purposes for which they collect, hold, use and disclose personal information.
- **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.
- **APP 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.

New requirement in the OP code — ceasing to use or disclose personal information upon request

The OP code will require organisations subject to the OP code 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. An individual may choose to use this when, for example, they do not want an organisation to disclose their personal information for the purposes of direct marketing. This requirement is not intended to amount to a 'right to erasure' of the personal information.

This will build on the existing requirements in APPs 12 and 13 of the Privacy Act which allow individuals to request access to, or correction of, their personal information. The new requirement will be carefully tailored to 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 authorised or required by or under another Commonwealth, State or Territory law or court or tribunal order; or
- are reasonably necessary to assist a law enforcement body undertake an enforcement-related activity; 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.

The new requirement recognises that, in some cases, it will be reasonable to take no steps to cease using or disclosing personal information following a request as it might not be practical to cease the use or disclosure. For example, if the organisation were required to keep some personal information in order to continue providing a service (such as billing information).

The Bill sets out the following procedural requirements for the request process (which are modelled on the procedural requirements in APP 12):

- 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.

New requirement in the OP code — children and vulnerable groups

The privacy practices of online platforms can be detrimental to children and vulnerable persons, including sharing data for advertising purposes, or engaging in harmful tracking, profiling, or targeted marketing. To date, details about how privacy protections under the Privacy Act should apply to children have been set out in guidance material from the Commissioner, rather than in the Privacy Act itself. 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.

The Bill will elevate protections for children and vulnerable groups by including stronger and more robust privacy protections as requirements in the OP code, as opposed to guidance.

For all OP organisations

The OP code will be required to set out how all the above provisions will apply specifically in relation to children or other groups of people not capable of making their own privacy decisions. In addition, the OP code will be required to make provision for how these individuals (or their parents, guardians or representatives) should provide consent for the collection, use or disclosure of personal information.

It is expected that in setting out how the above provisions will apply to children and vulnerable groups, stricter rules and stronger protections will be imposed in relation to OP organisations' handling of personal information of children and vulnerable groups.

For social media platforms

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 a child being defined as an individual who has not reached 18 years of age).

In addition to the requirements set out above, the OP code will require social media services to:

- Take all reasonable steps to verify the age of individuals who use the social media service; and
- Ensure that 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
- Obtain parental or guardian express 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 take all reasonable steps to obtain verifiable parental or guardian consent as soon as practicable.

The OP code may make provision in relation to what constitutes reasonable steps, or matters to take into account when considering whether the collection, use or disclosure of a child's personal information is fair and reasonable in the circumstances.

Optional requirements that may be included in the OP code

The OP code making powers provide for several requirements that would, if the Commissioner or OP code developer wish to use them, expand or clarify the obligations or procedures within the OP code. These requirements are optional to allow the OP code developer or the Commissioner to develop a code that is tailored, flexible and can respond to emerging issues.

These optional requirements would enable the OP code to:

- set out how one or more of the APPs are to be applied or complied with;
- impose additional (but not contrary or inconsistent) requirements to the APPs;
- provide mechanisms to deal with the internal handling of complaints;
- provide for the reporting of complaints to the Commissioner;
- provide for the reporting to the Commissioner about the number of end-users in Australia; and
- any other relevant matter.

Consequences for breaching the OP code

The Commissioner will have the power to investigate potential breaches of the OP code, either following a complaint or on the Commissioner's own initiative. The Commissioner's full range of enforcement powers will be available in the event that an investigation finds that a breach has occurred.

Developing the OP code: the code-making process

The process for developing the OP code will be based on the existing APP code and CR code-making processes.

Timeframes

After the Bill receives Royal Assent, the OP code will need to be developed and registered within 12 months. The Commissioner will register the OP code after it has been developed, and once the OP code has been registered it must be complied with by OP organisations.

How the OP code will be made

Industry will have the first opportunity to act as the 'OP code developer' and draft the OP code. The Commissioner will have the discretion to develop the OP code herself in certain circumstances.

Industry-developed code

The Commissioner may request that an organisation or a group of such organisations that will be bound by the OP code, or one or more industry bodies or associations representing such organisations, act as the OP code developer.

Before making such a request, the Commissioner must be satisfied that the industry participants are sufficiently experienced in the matters addressed by the OP code and sufficiently represent OP organisations as a whole to act as the OP code developer. The Commissioner may run a public process to help identify a suitable code developer. For instance, several industry bodies may jointly wish to approach the Commissioner to work together to jointly develop the OP code.

The Commissioner must make a copy of the request to develop the OP code publicly available as soon as practicable after the request to the OP code developer is made. The Commissioner's request must specify:

- the period in which the OP code developer must develop a draft code
    - the OP code developer must be provided at least 120 days to comply with the request. Within this time, the OP code developer will need to undertake public consultation on the draft OP code for at least 28 days before making an application to the Commissioner for registration of the Code.
- any other relevant matters that the Commissioner requires the OP code to deal with
- that the OP code is a binding instrument which contains enforceable obligations once registered.

Commissioner-developed code

As a result of the diverse range of entities captured by the definition of OP organisation, it may be difficult or impracticable for the Commissioner to identify a suitable OP code developer who is willing, who has the sufficient expertise to develop the code, and who sufficiently represents OP organisations.

If the Commissioner cannot identify a suitable OP code developer, or the OP code developer does not comply with the Commissioner's request to develop the code, or the Commissioner decides not to register the code that has been developed, the Commissioner can develop the OP code herself.

Once the Commissioner has developed a draft OP code, the Commissioner will need to publicly consult on the draft code for at least 40 days. During this time, the Commissioner may wish to bring the draft code to the attention of specific stakeholders, such as entities which will be considered OP organisations for the purposes of the OP code, as well as individuals or representative or advocacy associations. The longer timeframe compared to industry-developed OP codes reflects that industry may need more time to consider a Commissioner-developed OP code than one prepared by an industry OP code developer.

Code registration process

If the Commissioner decides to register an industry-developed OP code, or has developed her own OP code, she can then commence the code registration process.

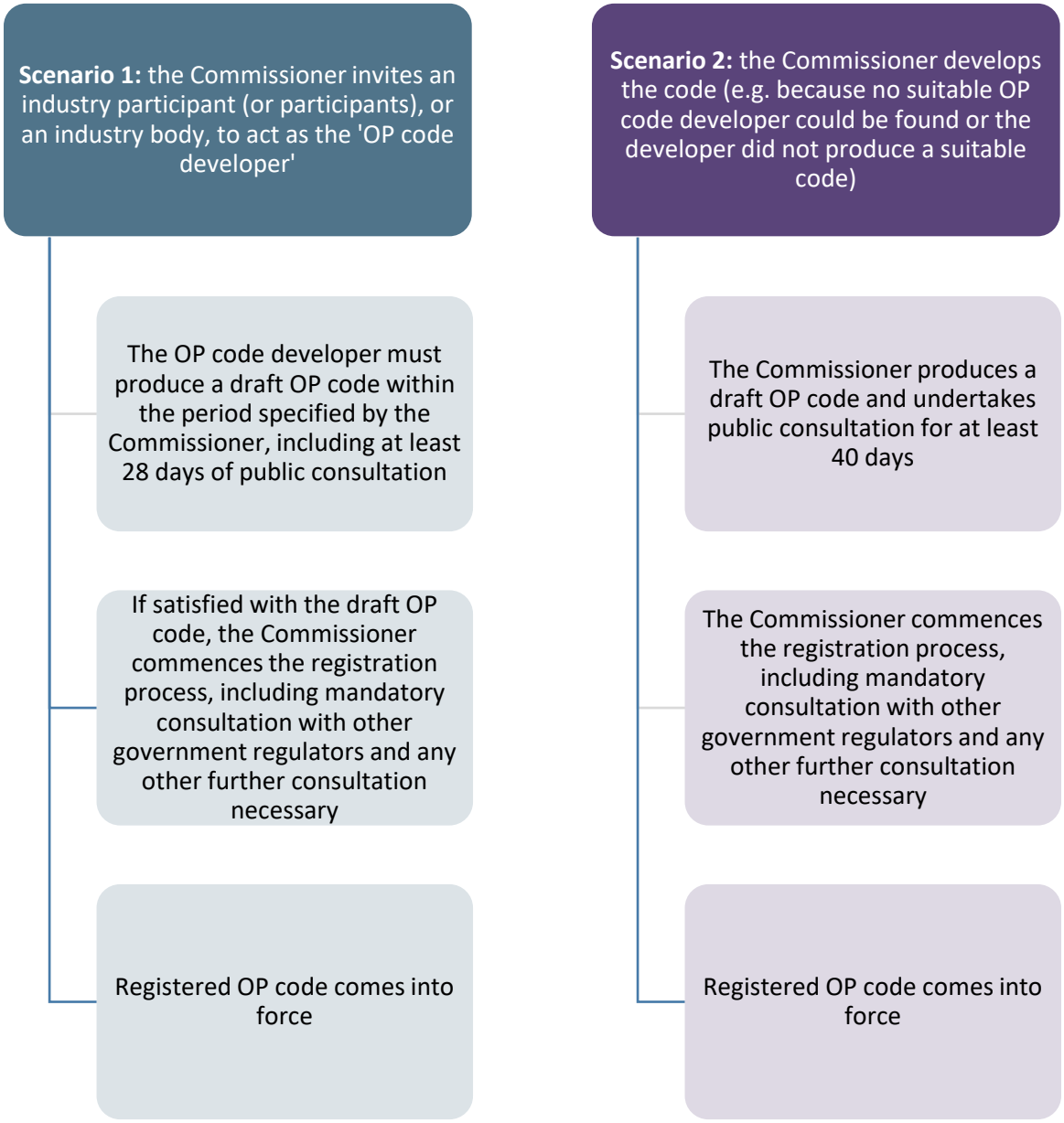
Before deciding whether to register the OP code, the Commissioner must consult and have regard to the views of the ACCC and the eSafety Commissioner, as Australian Government regulators that will also have relevant expertise about the OP code. This includes, for example, the eSafety Commissioner's expertise on what level of protection is appropriate for children and vulnerable groups. This recognises the intersection of privacy, competition and online safety matters in the digital environment and the importance of regulatory consistency. The Commissioner may also consult, and have regard to the views of, any other person the Commissioner considers appropriate before deciding whether to register the OP code. This could include, for example, the Commissioner undertaking further consultation on an industry-developed OP code. It could also allow further public consultation on a Commissioner-developed code after the initial mandatory public consultation period, if the Commissioner considers further consultation necessary.

The Commissioner may also consider any matters specified in relevant guidelines, including guidelines the Commissioner can make to assist the OP code developer to develop an OP code and the Office of the Australian Information Commissioner's (OAIC's) Guidelines for developing codes.

If the Commissioner declines to register an industry-developed OP code, the OP code developer will be able to seek review of that decision in the Administrative Appeals Tribunal. This is consistent with arrangements for APP codes and the CR code.

Diagram of code making process

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



When the OP code comes into force, and afterwards

The OP code will come into force once the Commissioner has registered it on a Codes Register which the Commissioner must maintain.

The registered OP code will be a form of delegated legislation known as a legislative instrument. This means the registered OP code will also need to be lodged on the Federal Register of Legislation (online at legislation.gov.au) and tabled in Parliament. The OP code will then be subject to the usual Parliamentary scrutiny process, including the possibility of disallowance through a vote in either house of Parliament.

Once the registered OP code comes into force, the Commissioner will be required to ensure that a registered OP code is always in place. This reflects that the OP code is essential to providing effective privacy protections for users of an OP organisation's services. This might involve:

- ***Replacing the registered OP code with a varied OP code as needed:*** variations to the OP code will involve a similar process to the OP code-making process set out above. In particular, industry would still be able to propose variations to the registered OP code for the Commissioner's approval, and consultation requirements would apply before the variation could occur.
- ***If no variations are made over the life of a registered OP code:*** making a new OP code to replace an expiring registered OP code. The registered OP code would follow the standard approach for legislative instruments of 'sunsetting' (expiring) after 10 years.

The Commissioner will also have a formal power to review the operation of the registered OP code. This is consistent with the Commissioner's powers to review the operation of APP codes and the CR code.

Other technical amendments to the Privacy Act to support the OP code

The Bill will make other amendments to the Privacy Act to support the operation of the OP code, and to ensure it operates in the same general way as APP codes and CR codes. These amendments include:

- Formally allowing the Commissioner to issue guidance material about the registered OP code.
- Expanding the Commissioner's existing assessment power to support assessments of compliance with the registered OP code, and empowering the Attorney-General to request the Commissioner undertake an assessment of a social media service's compliance with the additional protections for children.
- Allowing the Commissioner to grant a public interest exemption or temporary public interest exemption from the registered OP code, as with APP codes and CR codes and subject to the same procedural safeguards. This will require amendments to the Commissioner's existing public interest exemption powers, though these amendments are essentially only stylistic/technical in nature.
- Ensuring the Privacy Act's 'emergency declaration' provisions apply to the registered OP code in the same way they apply to APP codes in the event of an emergency or disaster.

If an organisation is subject to both the OP code and an APP code

The Bill will also provide that, if an entity is subject to both the OP code and an APP code, the OP code will prevail to the extent of any inconsistency between the two codes.

This provision has been included in the Bill for technical reasons, even though this kind of inconsistency is unlikely to occur in practice given:

- the relatively small number of APP codes in place at any one time; and
- the Commissioner's ability to deal with any inconsistencies during the respective code-making processes, or afterwards through a variation to the registered OP code or the relevant APP code.

If an organisation is subject to both the OP code and the Consumer Data Right rules

The Bill will provide that, if an entity is subject to both the OP code and the Consumer Data Right regime under the *Competition and Consumer Act 2010*, the Consumer Data Right rules will prevail to the extent of any inconsistency between the two codes.

This provision has been included in the Bill for technical reasons, to ensure that the strict rules specific to the Consumer Data Right regime continue to apply in relation to data handled as part of this system, consistent with the existing interactions of the Consumer Data Right system and the APPs and any APP code.

Part B: Enforcement and penalties for privacy breaches – Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021

These amendments will provide the Commissioner with an appropriate regulatory and enforcement toolkit to ensure the privacy regulator can resolve matters more efficiently and effectively, consistent with the public's expectations. These amendments are being progressed in advance of the review of the Privacy Act, as they complement the OP code and are necessary for the protection of Australians' privacy online.

There already exist a number of regulatory and enforcement powers available to the Commissioner under the Privacy Act. The Commissioner can, for example:

- direct an agency to provide the Commissioner with a privacy impact assessment,
- conduct an assessment of whether personal information is being maintained and handled by an entity as required by law,
- direct an entity to notify individuals at risk of serious harm, as well as the Commissioner, about an eligible data breach,
- investigate and make a determination on potential interferences with privacy, on the basis of a complaint or on the Commissioner's own initiative, and,
- commence proceedings to enforce an enforceable undertaking, determination, seek an injunction or apply for a civil penalty.

The Bill will strengthen the Commissioner's enforcement functions by:

1. Increasing the maximum civil penalty for a serious and/or repeated interference with privacy.
2. Creating a new infringement notice provision for failing to give information, answer a question or provide a document or record when required to do so as part of an investigation (with associated additional civil penalty provisions).
3. Creating a new criminal penalty for multiple instances of non-compliance.
4. Expanding the types of declarations that the Commissioner can make in a determination at the conclusion of an investigation.
5. Enhancing the Commissioner's capacity to conduct assessments.
6. Improving the Commissioner's information-sharing arrangements with relevant enforcement authorities and the ability for the Commissioner to disclose information in particular circumstances.

Current enforcement mechanisms under the Privacy Act

Investigations of possible interference with privacy of an individual

The Commissioner can commence an investigation into an act or practice that may be an 'interference with the privacy of an individual', by way of complaint to the OAIC or on the Commissioner's own initiative. Where

a complaint is made by an individual or a representative complainant that an act or practice is an interference with the privacy of an individual, the Commissioner is obliged to attempt conciliation of the complaint if there are reasonable prospects that conciliation will be successful. If satisfied that there is no reasonable likelihood that conciliation will be successful, the Commissioner may decide not to investigate, or investigate further, the act or practice subject to complaint. Where the Commissioner decides to continue investigating, the Commissioner can examine witnesses, require persons to produce information or documents and require them to attend compulsory conferences.

Power to make a 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:

- the complaint is not substantiated, or the act or practice does not constitute an interference with privacy,
- 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,
- the complaint is substantiated, or the act or practice does constitute an interference with privacy, and the respondent must:
    - take specific steps to prevent that conduct repeating or continuing,
    - perform an act or course of conduct to redress any loss or damage suffered by the complainant, and/or
    - pay compensation to a complainant.

Assessments of compliance with the Privacy Act

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 Act. This is a valuable regulatory/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 the 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, and the Commissioner may need to rely on other regulatory options.

Existing information sharing arrangements

Where the Commissioner suspects a particular offence has been committed (a tax file number offence, a healthcare identifier offence, an anti-money laundering and counter-terrorism financing verification or a credit reporting offence) or a contravention of a civil penalty provision under the *Personal Property Securities Act 2009* has occurred, the Commissioner must inform the relevant authority and provide them with a copy of the complaint.

The Commissioner can also provide any information or documents that relate to a complaint and are in the possession or control of the Commissioner for the purposes of transferring the complaint to an 'alternative complaint body' (i.e. one to which the Commissioner has powers to formally transfer complaints).

The Commissioner is otherwise bound by a secrecy provision in the *Australia Information Commissioner Act 2010* which generally limits her discretion to share information obtained during an investigation with other regulators. This can pose practical difficulties in cases where the Commissioner wants or needs to cooperate with other regulators.

New enforcement powers and penalties in the Bill

Increased penalty for serious and repeated interference with privacy

The ACCC's *Digital Platforms* report recommended that the maximum penalties of the Privacy Act be increased to mirror the recently increased penalties for breaches of the Australian Consumer Law (ACL).

For a natural person, the Bill increases the maximum civil penalty for serious and 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:

- $10,000,000;
- three times the value of the benefit obtained by the body corporate from the conduct constituting the serious and repeated interference with privacy; or
- if the value cannot be determined, 10% of their domestic annual turnover. The Bill sets out how to calculate turnover for the purposes of this provision.

These changes are consistent with maximum penalties under the ACL. Under Schedule 2 section 224 of the *Competition and Consumer Act 2010*, these penalties are $500,000 for a natural person and, for a body corporate, the greater of:

- $10,000,000;
- if determinable by a court, three times the value of the benefit obtained directly or indirectly and that is reasonably attributable to the act or omission; or
- if the value cannot be determined, 10% of the annual turnover.

A new infringement notice power and penalty for failure to give information

Under the Privacy Act the Commissioner may require a person to produce a document or record. For example, when conducting an investigation the Commissioner may require a person to provide information or produce a document that is relevant to the investigation. However, investigations can be delayed due to the failure of parties to respond to requests for information. Currently, section 66 of the Act creates a criminal offence where a person refuses 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 civil penalty provision to provide an alternative means of resolving these matters without resorting to the prosecution of a criminal offence or litigation of a civil matter. A separate criminal offence will be created for where a body corporate engages in

multiple instances of non-compliance.

When can an infringement notice be issued?

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 in relation to investigations. The amount to be stated in the infringement notice will be 12 penalty units for individuals, and 60 penalty units for bodies corporate — which, on the current penalty unit value, would result in a maximum penalty of $2,664 for individuals and $13,320 for bodies corporate. If the OAIC instead chooses to seek a civil penalty, the civil penalty for the infringement notice 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.

When can a criminal penalty be issued?

A criminal penalty may be issued if a body corporate fails to comply with the requirement to give information, or provide a document or record when required in relation to investigations, and this conduct occurs on multiple occasions and 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 from 100 to 300 penalty units for bodies corporate— which, on the current penalty unit value, would result in a maximum penalty of $66,600 for bodies corporate.

New types of determination

To complement the Commissioner's existing power to make a determination that a respondent must take specified steps to ensure conduct constituting an interference of privacy is not repeated or continued, the Bill will clarify that the Commissioner could also require the respondent to engage an independent and suitably qualified adviser to assist this process – including to review any relevant business practices or processes that contributed to the non-compliance, or the remediation of the non-compliance, and provide detail about their findings to the Commissioner. These provisions formalise the legal basis for a practice that the Commissioner has successfully used in multiple determinations in recent history.

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 and steps they have taken or will take to remediate the contravention, and to publish the statement and/or provide a copy to the complainant or, in the case of a representative complaint, to each affected class member.

Enhanced assessment power

The Bill enables the Commissioner to conduct an assessment of entities' compliance with the Privacy Act's Notifiable Data Breaches scheme, which commenced in February 2018.

The Commissioner currently has the power to assess an entity's compliance with certain parts of the Privacy Act, even in the absence of a breach of the Privacy Act or a complaint having been made. This is a valuable regulatory and educative tool to help identify emerging privacy issues. To assist the Commissioner to conduct assessments, the Bill will give the Commissioner a new information-gathering power for the purposes of

conducting an assessment of any kind. 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 notice can only be issued to the entity or file number recipient subject to the assessment;
- 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;
- 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.

Greater information sharing

Information sharing with law enforcement, complaint bodies and regulators

The Bill would also provide the Commissioner with the ability to share information or documents with the following:

- a law enforcement body;
- an alternative complaint body; and
- 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. This may occur when the Information Commissioner is holding information that relates to an investigation under both the Privacy Act and the receiving authority's framework.

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

- 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;
- 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; and,
- 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
- 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 agency (not a State, Territory or foreign body).

eSafety Commissioner as an alternative complaint body

To ensure that the Information Commissioner is able to share information with the eSafety Commissioner, the Bill would specify that the eSafety Commissioner is an 'alternative complaint body' under section 50(1) of the Privacy Act. This is necessary to allow information sharing to occur in the event of overlap between privacy complaints and complaints to the eSafety Commissioner – such as cyberbullying, cyber abuse and image-based abuse complaints.

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 acquired in the course of her privacy functions 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 information would be disclosed.

For all other permissible 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

The Commissioner would not be able to disclose information relating to an eligible data breach, unless the information was subject to an investigation following an interference with privacy of an individual. This is because the notifiable data breach scheme already has its own provisions regarding notification and publication, and is intended to encourage entities to volunteer information.

Extraterritoriality

Clarify the extraterritorial application 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 information from a source inside 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. Similarly, foreign organisations may collect personal information 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'.

The Bill will remove the condition 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.