BCA

Business Council of Australia

Online Privacy Bill

December 2021

Contents

1. About this submission

This is the Business Council's submission on the Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (the Online Privacy Bill). The Online Privacy Bill introduces a binding online privacy code and increases penalties and enforcement measures.

The Business Council represents businesses across a range of sectors, including manufacturing, infrastructure, information technology, mining, retail, financial services and banking, energy, professional services, transport, and telecommunications.

2. Key recommendations

The Business Council of Australia recommends:

1. The introduction of the bill and code be included within any future reforms to the Privacy Act, not progressed separately. If that is not possible, the scope of the Bill and Code should be narrowed to capture only those entities and activities of most immediate concern to the Government.
2. Government should consider options available to streamline reforms to simplify processes and practices for consumers and reduce unnecessary complexity and cost for business. This could include reforms in relation to the Consumer Data Right and eSafety Commissioner.
3. The definitions for each of the three types of regulated organisations should be revisited and cast more narrowly, to appropriately capture entities trading in consumers personal information and where there is a real consumer harm that has been identified, and to provide an explicit carveout for business-to-business platforms and interactions. Government needs to strike the right balance between enhancing protections where these are required to protect Australian consumers online from platforms trading in data and imposing regulatory burdens on an unduly broad field of organisations. There is, for example, no need to include 'large digital platforms' that do not trade in personal information.
4. The bill should specify the actions and practices that need to be regulated in line with the policy intent, rather than seeking to regulate all of the business practices of all regulated entities.
5. When requiring social media businesses to verify the age of individuals using their services, limit the requirement to "reasonable steps" in order to account for the potential for over-collection of data driven by a desire to take all steps that may be judged as reasonable, which would be contrary to the overall intent of the bill.
6. Do not proceed with the expanded declaration powers of the OAIC to direct regulated entities to publish a statement of conduct that constitutes an interference with the privacy of any individuals, given the data breach notification scheme requirements and potential risks to the privacy of other Australians that it may create.
7. Further consideration be given to how the requirement to cease using or disclosing personal information will work in practice, and whether, in the context of future changes to the Privacy Act, the need for collection of additional personal information and regulatory costs will outweigh by any potential benefits.
8. Provide a clear statement in the bill that where an organisation regulated under the code receives a request to no longer use their personal information, the organisation can cease providing a service to the objecting individual to the extent such use is necessary to provide the service. It should also provide clear exceptions for businesses to continue to use or disclose data in specific circumstances.
9. Industry be provided the first opportunity to develop the relevant industry code. The Commissioner's rights under s26KG should be limited to support this.

10. If the Government proceeds with the bill and code, a review of the operation of the code should be undertaken ahead of any further changes to the Privacy Act, to ensure it remains fit for purpose, or 24 months after it has been enacted

3. Overview

The Business Council supports measures that enhance the welfare of Australians, while allowing responsible businesses to operate in a way that balances the needs of all stakeholders and interests. The proposed changes are intended to protect Australians online by focusing on 'social media and other online platforms that trade in personal information' as originally announced in March 2019.

As the explanatory paper attached to the bill notes, the code will capture a very diverse range of organisations. The government has assumed that the total number of entities currently likely to be captured by the Bill numbers around 500. The number and diversity of businesses proposed to be captured, both now and in the future, means the scope and regulatory costs of the code must be carefully considered.

As it stands, the wide definitions will mean many Australian businesses will be in scope of the code including those that are neither social media businesses nor trade in personal information. If the requirements are onerous and only provides marginal gains to Australians, then we will be losing out on new, pro-consumer services or products, and deterring business investment. It could unnecessarily undercut the incentives for any entrepreneurs from investing their time and effort for new ideas in Australia.

The bill appears to capture a far wider range of businesses than originally intended by government or that is proportionate to any policy problems. The current scope could capture banks providing online services, telcos informing consumers about their usage, or supermarkets providing grocery deliveries. If the current definitions are retained, the number of businesses caught by the code will only grow as more businesses move online to meet consumer expectations.

It is also worth noting this bill is being introduced at the same time as the long-running and comprehensive review of the Privacy Act. Many of the possible changes to the Act, including the definition of 'personal information', will have substantial and real impacts on the operation of the proposed code.

This makes providing comment on the bill challenging, as the operation and potential costs and benefits may vary considerably depending on the outcomes of the review of the overall Act. It would be sensible to defer introduction of this bill and consider it as part of the wider review of the Act. Insofar as this is not possible, Government should focus on regulating those entities and issues of most direct concern to Australians online.

If the government wishes to proceed with this bill, the coverage of this bill should be revised. The Discussion Paper for the Privacy Act Review outlines possible alternative reforms that have not yet been selected and developed to a level of specification such that their practical effect and operation can be reliably assessed. Many of the matters the draft bill envisages would be required to be addressed in an OP code require covered entities to anticipate how complex areas proposed for substantial change in the Discussion Paper will be regulated under a revised Privacy Act.

Matters required to be anticipated and addressed by the draft code but canvassed for major reform in the Discussion Paper include the revised definition of 'personal information'; requirements for valid 'consent'; circumstances in which express consent must be sought and obtained; scope of operation of transparency requirements in relation to respectively privacy policies and privacy (collection) notices (that is, what must be addressed in each); the extent to which use of technical information for differentiated treatment of users will be regulated under the Privacy Act; whether there should be a broad form opt-out option for users of online services; and reasonable bases for exceptions from an opt-out option (i.e., any carve-down for reasonably anticipated or compatible uses or legitimate uses or interests).

These matters are not specified in the bill in sufficient detail to enable covered entities to develop a detailed OP code compliant with the stated requirements. This lack of detail and uncertainty as to future relevant changes leads to significant risk that the first round of code development will be protracted and contested and may not be successful. In any event, the first round OP code is likely to have a limited period of operation before covered organisations must fundamentally rewrite it to address new and changed requirements of a revised Privacy Act. The first-round code development process will need to be repeated in a second round of code development following Privacy Act reform.

As well as the cost of duplication of effort, the large number of covered entities and the diversity of their business interests and activities will add substantial complexity and cost. As a result, the true cost to covered entities in working on an OP code will be much higher than the estimates in the Government's draft Regulation Impact Statement.

If a first round OP code is to be required, an alternative approach would be to require development of OP code which specifies how covered entities should address current core APP requirements, applying current Privacy Act definitions and requirements as to the giving of notices (transparency) and as to consent, to the extent that the Government considers that these core requirements are not currently being appropriately addressed by some covered entities.

There should also be a clearly staged (phased) approach to development of the code, so that industry is not pre-empted by intervention by the regulator as a result of unrealistic expectations as to how quickly a code may be developed. At a minimum, industry should be allowed a clear twelve months from enactment of the OP Act to finalise a final draft code for submission to the IC for registration.

If the Government and the legislature is concerned that industry development may be delayed or stall due to complexity and range of covered activities and covered entities, the sensible way to address that concern is to narrow the range of entities and activities to be covered, and to require the code to address only those matters of application of current provisions of the Privacy Act that the Government and the legislature consider require more detailed elaboration in an industry code.

Scope of regulated entities

The exposure draft provides a number of definitions to identify the entities that will be captured by the code.

- This includes for ''organisations providing social media services' - any entity that allows 2 or more end users to share material or interact with each other
- data brokerage services - any entity that collects personal information that it discloses in the course of providing a service
- 'large online platforms' - any organisation that collects personal information about an individual in the course of or in connection with providing access to information, goods or services, and has more than 2.5 million users.

These are very broad definitions and will capture a far greater number of businesses than intended by government. The Regulation Impact Statement itself estimates that 150 social media providers, 85 data brokerage services, and 265 large online platforms would be covered by the bill.

The wide definitions of 'large online platforms' would capture any organisation that provides online access to their services (banking, booking flights online, account information about electricity/gas/water usage etc) where they have more than 2.5 million customers.

If a bank collects personal information in the course of providing a banking online service, or if a supermarket collects personal information in the course of providing goods via online grocery shopping, or if a telco collects personal information through an app that provides information about the usage of their telecommunications service, then these entities would appear to be caught within the definition. This will create substantial perverse incentives (not least for companies to not seek to grow in Australia), and does not align with the Government's

intention as expressed in its March 2019 media release or the Explanatory Paper. Based on this, we understand these types of entities are not intended to be captured and therefore, the definitions in the bill need to be updated to clarity this.

The quantity of users will also need to be more explicitly defined, including how Government arrived at the number of the 2.5 million users and how this should be calculated. Does this mean 2.5 million total users, unique users, active users, or concurrent users? Each of these will pose different challenges for businesses and individuals to navigate the regulation. If the 2.5 million users are intended to be unique, for example, entities may be required to capture additional personal information from individuals to establish this and de-conflict any duplicates. Conversely, should the definition of "personal information" in the Privacy Act be amended to encompass additional information such as IP addresses or similar metadata types, there is a risk that any platform, irrespective of whether it collects other personal information, will be caught by the code, even if trying to operate a site without requiring identification of individuals.

Similarly, the definitions of 'data brokerage services' and a 'organisations providing social media services' is are very wide and unclear. The current definition of 'data brokerage service' refers to an organisation that collects personal information about an individual for the sole or primary purpose of disclosing that information (or information derived from that information) in the course of or in connection with providing a service'. On a strict reading the words 'information derived from that information' suggest that the definition is intended to expand beyond personal information to also capture de-identified or anonymised information derived from information collected from individuals. As this reading does not align with the stated objective of the Bill, we assume it is incorrect and see value in this being clarified.

The definition of 'social media services' is also overly broad. It does not have a floor on the number of users, so conceivably any service that allows only two end-users to interact or post material would still be regulated under the code. Any definitions need to be carefully considered, to not inadvertently disincentivise entities who may wish to offer new services with clear consumer benefit in the future or create an unnecessary regulatory burden for new, innovative services.

We recommend the definitions be revisited and cast more narrowly, to appropriately capture those business functions and entities where a real consumer harm has been identified. Explicit carveouts should be provided for business-to-business interactions and platforms.

Scope of regulated activities

For all of the entities covered, the Bill also brings into scope all of their activities. The only exception is if section 26KC(9) is used by the code developer or the Commissioner to take specific activities of a covered entity out of coverage. Including all business activities within scope is disproportionate to the problem the Government is trying to solve. It will make it much harder for potentially covered entities to negotiate and agree a code, given the range of activities that need to be considered will be immense. Instead of starting from the basis of covering all activities and working with exclusions, the bill should specify harms sought to be prevented and consequently the actions and practices that need to be regulated. Only those activities and practices by covered entities, and the uses of personal data about individuals derived from those activities and practices, should be within the bill's coverage.

We also recommend that the government to take an overarching view of reforms in related areas including the Consumer Data Right and the eSafety Commissioner in order to reduce complexity for consumers and business.

New requirements to cease using or disclosing personal information

The code will require organisations to take reasonable steps to not use or disclose, or to not further use or disclose, an individual's personal information upon request from that individual. This overlaps with proposals made in the Privacy Act Review discussion paper.

These requirements will impose substantial additional regulatory costs for businesses, given it will affect entire businesses. This is particularly the case given the potential for the definition of 'personal information' to change following the ongoing review of the entire Privacy Act.

Further, the explanatory paper attached to the bill indicates that one of the reasons for including the right to object relates to direct marketing and providing an avenue for individuals to object to their data being used for direct marketing purposes.

The wider application of this 'right to object' should be carefully considered, particularly in how it will affect advertising supported services. Australian people and businesses benefit from access to services funded by personalised advertising. This is particularly the case for small Australian businesses – 71 per cent of Australian small businesses that use personalised advertising reported that it is important for the success of their business.[1]

Personalised advertising are also critical for businesses – large and small – to reach new customers and grow. BCG found 80 per cent of marketers reported an increased ROI over the past three years, particularly from better technology that enabled the personalisation of advertising.[2]

This has been even more critical through the recent pandemic as all businesses and consumers have had to quickly pivot to the digital economy. It enables businesses to reach new markets and create more jobs.

The right to object should also allow businesses to cease providing a service if a consumer objects to their personal information being used for advertising. Requiring a business to fundamentally change its business model to respond to a consumer objection is untenable, particularly where there are readily available alternative services if a consumer objects to advertising supported services.

Further, the opt-out is qualified only by "such steps (if any) as are reasonable in the circumstances". This qualifier will be practically impossible to give effect in the OP code, because of the range of activities and range or entities to whom the Government proposes that the code relates. It is not clear what may be regarded as reasonable bases for exceptions from an opt-out option (i.e., carve-downs for reasonably anticipated or compatible uses or legitimate uses or interests).

It will be important that the bill include provisions for an organisation to continue to use or disclose information where there are legitimate requirements, such as to complete or give effect to a contract, to comply with other laws, or for safety, security or integrity purposes.

We suggest that such an uncertain and broadly drafted opt-out should not now be required in advance of the legislature enacting reforms as canvassed in the Discussion Paper.

We recommend consideration of how this is requirement will work in practice, and particularly whether, in the context of future changes to the Privacy Act, the regulatory costs will be outweighed by any potential benefits. However, if government includes this component of the bill, it should be focused on those businesses and areas requiring urgent attention to meet the expectations of Australians. Taking a more expansive approach imposes an unnecessary financial burden on business and has the potential to cause confusion in the longer term.

If the government proceeds with this requirement, the legislation should clearly state that, where an organisation regulated under the code receives a request to no longer use their personal information, the organisation can cease providing a service to the objecting individual to the extent such use is necessary to provide the service. It should also provide clear exceptions for businesses to continue to use or disclose data in specific circumstances (such as those noted above).

Further, section 26KC(2)(h) should make it clear that uses and disclosures of effectively anonymised data are outside of scope of coverage of that provision. Effective anonymisation and use of effectively anonymised data is consistent with good privacy-by-design (PbD) principles and good PbD data handling practices.

[1] https://www.facebook.com/business/news/new-insights-on-personalized-ads-and-social-medias-impact-on-small-businesses
[2] https://www.bcg.com/publications/2020/leveraging-european-marketing-ecosystem

Requirements for social media platforms

The bill will create new requirements for regulated entities. This includes requiring social media businesses to take all reasonable steps to verify the age of all individuals who use the social media service.

The 'reasonableness' requirement will be critical here. It is possible entities will be required to take steps that would be anti-privacy, as it would place the onus on businesses to collect further information on individuals to verify their age beyond what they were already doing. We recommend the government considers limiting the requirement to "reasonable steps" in order to account for the potential for over-collection of data driven by a desire to take all steps that may be judged as reasonable.

Disclosure by Privacy Commissioner of information acquired through investigations

Proposed section 33B(1) would empower the Commissioner to disclose information acquired by the Commissioner in the course of exercising powers, or performing functions or duties under this Act if the Commissioner is satisfied that it is in the public interest to do so.

There is no limitation as to the nature of information that may be disclosed. Accordingly, disclosed information might include any information supplied to the Commissioner in the course of an investigation, regardless of whether that information is contested as to accuracy, completeness or relevance.

There is no requirement of prior consultation with the person or entity that provides the relevant information or to whom the information relates.

There is no requirement for the Commissioner to consider proportionality or to balance benefit to person or entity that provide the relevant information or to whom the information relates against, merely to "have regard" to the matters specified in proposed section 33B(4).

Section 33B(1) should be amended to require the OAIC to consult with affected entities ahead of disclosing any information, and to have regard to the proportionality of any information released. The types and nature of the information the Commissioner can release should also be further prescribed to reflect the policy intent of this section of the bill.

Declaration of interference

The OAIC may investigate a complaint or an act or practice that may be an interference with the privacy of an individual. If this investigation finds it to be substantiated, the OAIC's determination may now also include a declaration requiring the respondent to prepare and publish (or otherwise communicate) a statement setting out a description of the conduct that constitutes the interference with the privacy of an individual and the steps (if any) undertaken or to be undertaken by the respondent to ensure that the conduct is not repeated or continued.

The respondent will be required to publish a statement in accordance with the Declaration made by the Commissioner. While the matters specified in the Declaration (made by the Commissioner) need to be "reasonable and appropriate", we are concerned the publication of system and process vulnerabilities (including any steps taken to ensure conduct isn't repeated or continued) risks providing individuals or groups who will use this information to identify and exploit existing or new vulnerabilities.

The purpose of this declaration is also unclear. It is likely entities will already be required to make a notification through the mandatory data breach notification scheme to impacted individuals so they can take appropriate mitigation action. The specific benefits of this declaration should be re-examined – it is not clear how this will provide additional benefits to Australians, and whether these benefits would outweigh both the risks (identified above) or the additional regulatory costs.

Development of the code

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.

The code may be developed by either industry or by the Commissioner, where the Commissioner cannot identify an entity who is willing and has sufficient expertise to develop the code, and who sufficiently represents the regulated entities.

We support industry being provided the opportunity to develop the code in the first instance. Given the wide scope of the code, it may be necessary for a coalition of organisations to develop the code, rather than a single industry body (or even two, as suggested in Regulatory Impact Statement – though it is unclear why the RIS envisages two code developers when there is to be only one code). It would be helpful for government to provide further detail on the next steps for the development of the code, if the legislation were enacted, as the current approach appears to condemn an industry developed code to failure due to the wide range of organisations and activities that need to be covered.

We recommend the bill be amended to clearly allow industry 12 months to develop and submit a code. If, as the discussion paper suggests, the diversity of organisations and activities to be regulated make it impossible to identify a code developer, then this should be cause for government to narrow the range of entities and activities to be regulated, as we have highlighted above.

BUSINESS COUNCIL OF AUSTRALIA

42/120 Collins Street Melbourne 3000 T 03 8664 2664 F 03 8664 2666 www.bca.com.au