Submission to the Australian Federal Government's consultation on the Privacy Bill

Authors

This response is written on behalf of the Platform Pedagogies reading group. *This response is not affiliated with any other groups or institutions; we are writing as in a private capacity, as a group of academics and a community of intellectual interest.* We seek to explore the interaction of learning and online spaces; exploring how each impacts the other and how we can imagine new, progressive futures online. More information can be found at https://platformpedagogies.com/.

Gavin Duffy PhD student - School of Education (Apps in Schooling), Deakin University

Dr. Robbie Fordyce Lecturer - Communications and Media Studies (Big Data/Quantitative Analytics and Research Methods), School of Media, Film & Journalism, Monash University

Signatories

A/Prof. Radhika Gorur - Associate Professor of Education (Pedagogy and Curriculum), Deakin University

Dr. Alexia Maddox - Research Fellow (Blockchain Innovation Hub), RMIT University

Prof. Julian Sefton-Green - Professor of Education (New Media Education), Deakin University

Dr. Andy Zhao - Research Fellow (Digital Childhoods), Deakin University

Dr. Kate Mannell - Research Fellow (Digital Childhoods), Deakin University

Dr Luci Pangrazio - Alfred Deakin Postdoctoral Research Fellow (Centre for Research in Educational Impact), Deakin University

Summary

We are responding to the request for submissions on the exposure draft of the Online Privacy Bill and consultation Regulation Impact Statement, as presented on the website for the Australian Government Attorney-General's Department.

This response is motivated by concern over a substantial disconnection between the proposed goal of keeping children safe online, and the proposed solutions which do not currently include any way to do this, instead including many factors that are retroactive to children's safety. Within the Explanatory Paper (EP) and Regulation Impact Statement (RIS) for the Bill, there are several sections addressing how the Bill should work for 'children and vulnerable groups'. This is not, inherently, a negative: it is perfectly coherent that children and vulnerable groups may need extra legal protections online (as they do offline). It is more specifically how the stated aims of keeping these groups 'safe' online are to be implemented, according to the EP and RIS, as well as some of the justifications for these actions, with which we would like to engage.

Overview

Our observations

We are principally concerned with four primary elements, for which we see substantial barriers to implementation. Importantly, we wish to highlight the key contradictions in terms of the goals of the legislation and the proposed implementation strategies. We want to highlight how the proposed legislation will fail to protect citizens, and instead introduce new risks which have not been anticipated in the legislation. We are concerned, moreover, that, absent substantial protections for citizens, the proposed legislation will introduce a 'chilling effect' on free and public discourse in Australia.

List of Our concerns

- In terms of impacts on children, we see a substantial risk in requiring those under 16 years old to disclose personal identity details to commercial platforms in order to access those platforms.
- Media access and media literacy are highly varied across Australia. Because of this, there will be uncertain outcomes including potential uneven exposure to regulation across populations and demographics, furthering the digital divide. The unevenness of outcomes is increased by the responsibilisation of parents around their child's online activity, while reducing the responsibility of the state.
- We have a series of methodological concerns about how the legislation is being constructed, and about the consultative process. This includes large (often overseas) companies determining the very policy intended to govern their behaviour. The storage of any data collected as a part of the Privacy Bill also remains unclear.
- The legislation implements 'tracking as a solution', and this has dubious value.
    - In terms of prevention, it has a marginal role.
    - In terms of legal remedy to breaches, the value of tracking data will be much higher for those with greater financial resources and social capital. Children as individuals are unlikely to have any capacity to commence legal proceedings, which extends to those who are less wealthy or less well-educated.
    - Vulnerable communities are already subject to substantial tracking of their personal and private lives by government agencies such as Centrelink. The draft legislation may increase this tracking, expanding it in the digital space, again exacerbating existing social inequities.

Our method

Our observations are informed by our career expertise, as noted below, and are supported by two key scientific research methods. The first is our ongoing review of industry reports and academic scholarship on the topic; we have provided a selection of resources in our bibliography that represents the components of our review that most tightly align with the legislation. The second is the use of policy analysis methods; our research group has pioneered approaches in applying policy analysis to data contexts, publishing this work in world-leading peer reviewed academic journals (journals classed as ‘Q1’ by independent review); this expertise has been used in this report. In the interest of brevity, specific methodological approaches will be supplied on request.

Our expertise

We are researchers based at Australian universities, with expertise in studying the social impacts of technologies and the production, circulation and storage of personal data. Our expertise is derived from our substantial career experience as analysts and researchers, and is supported by our research environments, which includes the Australian Research Council-funded Centre for the Digital Child and the Monash-based Automated Society Working Group and the RMIT-based Blockchain Innovation Hub. We are thus well positioned to comment on this draft legislation, especially in terms of its impacts on children.

As stated previously, we offer this submission as experts from the Platform Pedagogies reading group. This submission is not intended as the official submission from any institution; we are a community of intellectual interest, submitting a response in a private capacity.

Response to draft legislation

Methodological limits of the proposed legislation

We have several key concerns about the way that this legislation has been developed in terms of the process of creating the policy.

There is no substantive or dedicated attempt evident in the documentation to take account of Aboriginal/Torres Strait Islander/Indigenous Australian voices on this matter. Due to historic targeting of these groups in online contexts, by individuals who were not anonymous, and the expectation that this will likely continue after the legislation, we note with concern that there has been no substantial attempt to include these groups. The lack of considered engagement with Aboriginal/Torres Strait Islander/Indigenous Australians is a failing of the legislation.

The consultation is wholly online and not substantively advertised to the community. Additionally, the consultation documents are only available in English, excluding culturally and linguistically diverse communities. Because of this, those with limited media literacy and those with limited knowledge of government systems, who will be substantially affected by these developments, will have no voice in this process. The lack of considered engagement with the community is a failing of the legislation.

There appears to have been no dedicated consultation with advocacy groups or researchers on the impacts of this legislation on children. For example, the national Australian Research Council-funded Centre of Excellence on the Digital Child was not involved in any discussions in crafting this legislation. The lack of considered engagement with the experts and advocates is a failing of the legislation.

The details of the legislation are being left to private commercial platforms to develop. This in essence passes over the governance of citizens to private corporations. It is highly unlikely that the Online Protection Code (OP Code) Developer will be an organisation that is Australian-owned. Few of the corporations that meet the criteria of the legislation will house any data on Australian children in servers within Australian borders, with most of this data being housed in other legal jurisdictions. There are no clear requirements about what will be done with private data after it has been obtained.

The legislation has no clear and objective criteria for the selection of the OP Code Developer, and it is unclear how the legislation will be assessed as being of good quality and having outcomes appropriate to civic needs.

Criticisms of problem construction

The problem that this draft legislation seeks to address is most clearly articulated on page 4 of the Regulation Impact Statement, where it is framed as:

- Excessive capture of personal data in online contexts.
- Individual consent and agency with respect to digital platforms
    - A lack of clear consent
    - A lack of bargaining power with respect to terms and conditions
    - A lack of media literacy around privacy and settings
- Governance processes for penalty and enforcement measures
    - Insufficient penalty units for breaches relative to community expectation
    - Insufficient enforcement measures for forcing disclosure from companies
    - Lack of tools for assessment of and intervention in investigation measures and outcomes for the Commissioner
    - Information sharing from the Commissioner
    - Jurisdictional issues around global trade in data

This is a complicated series of issues. The core of these issues is that private companies capture substantial volumes of data on individuals; that this is done without clarity for individuals in terms of what the scope of this capture is or what could be done about it; and generalised concerns around lack of civic knowledge about platform interfaces. Further, there is concern that this data is warehoused in jurisdictions outside Australia's direct legislative control, and that the Commissioner and the relevant governing bodies have few tools to manage these problems.

Yet the solutions that are presented in the draft legislation do not address these problems adequately. We address these below.

Excessive capture of personal data in online contexts

The draft legislation requires individuals to provide more personal information, particularly information that identifies someone as a legal subject of Australia, which only exacerbates the matter of excessive data capture.

This is seen most evidently in the draft legislation's desire for 'stronger and more robust privacy protections' for young people. We applaud the strong desire to provide additional protections for young people, such as requiring certain acts and practices (such as default privacy settings) and limiting certain acts and practices. The latter includes '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' (RIS, 16). Reducing the amount of data collected by digital companies on children, on the face of it, appears sensible and uncontroversial.

However, it is how these protections are to be implemented which poses an issue. The draft legislation proposes that social media platforms, 'take all reasonable steps to verify the age of individuals who use the social media service' and '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'. This age verification process would likely exacerbate, rather than solve, privacy issues.

In order for these 'more robust privacy protections' to have much effect, they must be strict and systematic. This would likely require a system of age verification with real-name ID, recognised by both the government and companies subject to the OP Code. Thus, we are concerned that, under the guise of online child-safety, a system of mandatory government identification and a real-name internet would emerge. We view this as a risk to individual privacy online for all, rather than protecting privacy.

Without such a systematic measure, it becomes difficult to see how any age-based requirements could be enforced. Even within the EP and RIS, there is the suggestion that a social media service may gain 'new information to suggest an individual previously believed to be over the age of 16 was in fact not'. If this situation occurs and no strictly regulated means of age-verification is in place, this under-16 individual could simply make another account and avoid future indications of their age. The conception of parental/guardian consent for those under-16 therefore rests on a notion of a government enforced, real-name internet or is purely symbolic.

If it is the former, we fear that the Online Privacy Bill is a risk to one's private online presence. A real-name internet allows for a much more robust system of tracking and data collection than we currently see, as well as making this tracking easier; an identifiable data-profile of each person would be created and centralised. This could be of particular risk to those who *are* members of vulnerable groups that are already subject to undue surveillance e.g. Aboriginal/Torres Strait Islander/Indigenous community members, as noted by Bielefeld and Henne (2021). With the RIS noting that online privacy practices can be detrimental to such groups, particularly through

profiling, it is important that this regulation itself does not exacerbate the issue further.

If it is the latter, then we fear the Bill will have no real benefit for children and place the blame for any future errors upon their parents or guardians (discussed further below). Regardless of the outcome, this proposal within the draft legislation is clearly unfit for purpose.

Individual consent and agency with respect to digital platforms

While we agree that there are substantial limits to the Privacy Act (1988) in terms of the current state of the digital economy and online culture, we have specific concerns about how these limits are understood as problems, and with how these 'problems' are solved.

The draft legislation is unclear, but appears to require individuals to consent to providing a commercial platform with their personal documents and agreeing to the platform's terms and conditions; if not, they have no option but to leave the platform. This means that the draft legislation will legalise platforms to engage in coercive consent with regard to personal data. As it stands, the requirements that the draft legislation makes of platforms are unclear in this regard. We read the current draft legislation as allowing platforms to retain personal data, as well as information derived from personal data, even after someone has left the platform. Furthermore, the legislation does not address the issue of pixel or cookie-based tracking, such as implemented by the Facebook pixel, nor addressing users consenting to one service provided by a platform while refusing others (such as consenting to Instagram but not Facebook). This means, in the current iteration of the legislation, users may have their data collected by a social media service *other* than the service they have signed up to, due to elements embedded into a website or data shared with a parent company. This data (or even meta-data) can be used to construct a virtual person (as opposed to a legal person) to track users. This lack of clarity around a platform's obligations with regard to user data and the sole focus on legal persons (rather than virtual persons) potentially offers platforms a means of skirting the draft legislation's proposals.

In regard to children in particular, the draft legislation eschews this concern in favour of an individualised approach to consent, responsibilising parents and guardians for their children's engagement with online platforms. In both the EP and RIS, the role of parents/guardians/representatives is dealt with. Specifically, their role in the draft legislation orients around 'how these individuals should provide consent for the collection, use or disclosure of personal information' (EP, 11). The RIS notes the parental role of consent-oversight and goes further, citing the eSafety Commissioner's May 2018 '*State of Play - Youth, Kids and Digital Dangers'* Report which, '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' (RIS, 6). Additionally, the RIS states that where an

individual under 16 (i.e. a child, according to the Bill) is found to be using a social media service already, 'the social media service must obtain verifiable parental or guardian consent as soon as practicable' (RIS, 16).

While undoubtedly parents and guardians have a role to play in their child's use of digital devices/social media services, we take issue here with the seemingly sole responsibility they bear within the EP and RIS. This is particularly the case for the claim that parents and guardians should play a key role in assessing a child's ability to deal with online content. Within the EP nor the RIS, there appears to be no commitment to critical digital literacy being championed by the Federal government, or State institutions.

This responsibilisation of the caregiver (and tacit de-responsibilisation of the state) assumes both a technical and material proficiency which a parent or guardian simply may not have i.e., caregivers themselves may not fully understand what is online or possess the digital devices in the home with which to teach their children about online behaviour. Conversely, education departments across Australia have a focus on the digital within their curriculum (e.g. Victorian Curriculum and Assessment Authority, 2021; Education Standards Authority NSW, 2021) and the ability to provide (or attempt to provide) all students with equitable access to this education. In abdicating the role of the state in helping children learn about digital spaces, the EP and RIS take for granted that all parents will have the time and ability to deal with this issue. This responsibilisation of parents will undoubtedly lead to individualised and lop-sided understandings of online spaces amongst children; favouring those with middle-class and tech-savvy parents and entrenching the existing digital divide (Thomas et al, 2020).

Enforcing penalty measures

The draft legislation notes the lack of enforcement measures for the Commissioner against platforms in breach of legislation, yet invites platforms to rewrite this as the OP Code. The EP (12) briefly outlines the proposed development process for the OP Code: '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 but this is treated as a secondary (and non-preferred) option. This is contradictory in terms of civic outcomes and in terms of creating progressive and fair legislation.

This focus on (and preference for) an industry-developed code reflects some of the underlying values within the draft legislation, particularly the desire to 'enhance privacy protection… *without unduly impeding innovation within the digital economy'* (EP, 4, emphasis added). The RIS reiterates this, seeking a balance between 'empower[ing] consumers… and best [serving] the Australian economy' (RIS, 3). There appears to be a desire to marry the concerns of the public in the wake of data-related scandals such as Cambridge Analytica (mentioned in both the EP and RIS) with the interests of businesses. However, the details around the development

of the OP code remain unclear. There is no detail on the criteria for a 'suitable code developer', for example. It is noted that this *could* be a singular 'industry body' who would go on to determine government regulation for an entire sector.

While we approve of the requirement that the eSafety Commissioner must be consulted on any industry-developed code, this requirement is in place to consider the intersection of 'privacy, competition and online safety matters'. As noted above, the current youth-oriented propositions in the draft legislation may actually pose a challenge to any future online privacy. Secondarily, 'competition' (and the language of the market generally) remains a primary concern of the draft legislation. This is reflected in the existence of an appeals process for any industry bodies who have their OP Code rejected but no equivalent body for objections from the public.

Additionally, there appears to be little transparency around the storage of either the data collected by companies or the data collected as part of the OP Code. Within the two documents (the EP and RIS), the only mention of data storage is that of extraterritorial data i.e. data collected by a company which is not incorporated in Australia. The RIS acknowledges that data about Australians, which is collected by companies outside of Australia, 'has the potential to impede the Commissioner's ability to take effective regulatory action against overseas companies' as it currently stands. The current Bill seeks to rectify this only by making overseas companies 'more clearly subject to the Privacy Act', rather than exempt from the Act as they are currently (EP, 23). The current draft legislation therefore still does not require that Australian data is stored in Australia.

Similarly, there is no mention of how any data collected by, or submitted to, the Commissioner will be stored. Within the EP and RIS, there is no indication that this data will be stored in Australia or that there will be specific data storage standards applied to it. It is possible, then, that this is something to be determined by the industry body/bodies which will draw up the OP Code, allowing private companies to determine the data storage requirements which regulate their data collection. Once again, when the posited concern around young people's data is its misuse by the private companies that gather it, the lack of clarity in the current policy documents around how this misuse will be eliminated, or at least minimised, appears problematic.

Overall, it appears that the OP Code will function as a form of public-private partnership, with business leading government on how to regulate business. Under these circumstances (and in light of Williamson and Hogan's (2020) critique of such public-private partnerships in EdTech in the context of the COVID-19 pandemic), it is once again difficult to imagine the OP Code as fundamentally altering the current data-collection processes. While the privacy rights of youth are presented as pivotal for the Privacy Bill, functionally the guidelines for the OP Code seek to merely acknowledge 'community beliefs and expectations' (RIS, 3) while maintaining a status quo of data collection, albeit with more robust fines. This calls into question the suggested concern for the protection and privacy of youth in digital spaces, with this concern again seeming to act as a means to an (economic) end, rather than as an end in itself.

Recommendations

We are strongly supportive of legislation that seeks to revisit the pressing matter of public and individual use of digital technology. We consider several of the themes to be important to Australia's digital future. We do, however, have significant concerns regarding the way the draft legislation identifies the problems, as well as the proposed solutions. We offer the following recommendations.

That children and their safety not be used as a mechanism or justification for introducing privacy eroding legislation. This legislation does not make children safer. This is particularly concerning to us; younger persons engage with more platforms, have extremely divergent media literacy, substantial socialisation pressure, and less knowledge of personal agency, legal remedy and consent. They have different life priorities from older individuals, and likely have less concern or knowledge of data as a source of value. Younger persons are more likely to be disadvantaged by this legislation due to these factors. Any legislation put forward that will impact young people's online experience must include young people in its design, while actively avoiding the implementation of a real-name internet.

That any legislation be evidence-based. Currently the evidence for this legislation is limited, and some of the cited reports have been misinterpreted. We particularly note that there are ungrounded assumptions about the role of anonymity in making social media 'safe'. We recommend that the youth used as a basis for much of this legislation are consulted to build empirical evidence. This takes inspiration from the 5Rights Foundation (2021), which advocates for (and contributes to) young people's inclusion in the formation of digital governance. Rather than utilising data from the eSafety Commissioner's 2018 Report (in which students were questioned on issues such as alienation and loneliness, not strictly on privacy or data collection), it would be of use to establish a working panel of young people to discuss their views and learn from their experiences in relation to online privacy.

That the legislation be paused until after a genuine attempt has been made to substantively canvass the impact of this legislation on affected and marginalised populations. We suggest that consultations are set up with women's rights organisations with an online focus, independent online privacy organisations, Aboriginal/Indigenous/Torres Strait Islander groups, disability groups, consumer advocacy groups, community organisations representing those of diverse cultural heritage, and legal advocacy groups. Such an intersectional approach to the draft legislation is vital, as these privacy rights will impact a range of groups. This approach is advocated by Lowitja Institute's (2021) *Close the Gap Report.* This report notes the important role played by Aboriginal/Torres Strait Islander/Indigenous youth and young leaders in addressing issues relating to their land, both in the present and for the future. We would like to see these groups empowered through their input being heard by institutions of governance, and being given at least the same level of

respect as afforded to the industry bodies upon which the EP and RIS so heavily focus.

That any consent procedures be implemented in a way that genuinely empowers individuals and communities. Users should be provided with greater capacity to decide on how their data is captured by platforms, greater capacity to cease that relationship, and greater capacity to modify that relationship. This should be implemented whether users are young or old, media literate or not, wealthy or not.

That the market not be considered a mediator for bargaining power. The market leaves wealthier and more literate people and populations with more bargaining power, and it is therefore inequitable.

If the objective of offering legal remedies to online abuse is serious, then **private individuals should be provided with easy access to government funds to commence legal proceedings**. At present, we see wealth as a substantial barrier to individuals' capacity to launch legal action.

That the focus on legal persons does not lead to an ignorance of the privacy issues that arise from implied or virtual persons. The draft legislation primarily attends to the construction of legal persons and their digital traces. However, a great deal of online data extraction is not at the level of the personal (i.e. from an individual who directly identifies themselves in a consenting manner). A vast amount of data is extracted from implied or virtualised persons, through the use of identifying markers such as cookies, IP addresses, or digital fingerprints. The legislation does not address the way implied users are constructed on commercial databases using this proxy information. Indeed, from a commercial perspective, the value of implied data - of what a person is probably doing off the platform - is far more valuable than any actions that take place within the platform itself. The fact that there is no mention of this, no framework for refusing to consent, and no attention to remedies for it is a major oversight. This is surprising given the substantial impact of legislation such as the EU's GDPR which has demonstrated that ambitious legislation to protect individuals in precisely this area can be implemented.

That a limited number of private companies not be empowered to write the legislation governing online privacy and personal data. While sector-based self-regulation can be an effective procedure for managing industry-specific tensions, this draft legislation goes beyond self-regulation to provide an OP Code Developer (which may be one or many organisations, and may be primarily based outside of Australia) with the ability to write legislation about its primary commodity: data about private citizens. The draft legislation as it stands would seem to cover everything from legal remedy to consent procedures, to obligations by the platforms. This is far beyond self-regulation. If this is implemented, the well-known wicked problem of policy inheritance will leave Australians burdened with legislative mechanisms into the future.

Bibliography

5Rights Foundation. (2021). About 5Rights Foundation. Available from: https://5rightsfoundation.com/about-us/ (accessed 26/11/2021).

Australian Government, Attorney-General's Department. (2021). Explanatory paper: Privacy legislation amendment (enhancing online privacy and other measures) bill 2021. Available from: https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/user_uploads/online-privacy-bill-explanatory-paper.pdf (accessed 26/11/2021).

Australian Government, Attorney-General's Department. (2021). Enhancing online privacy and other measures: Early assessment - regulation impact statement. Available from: https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/user_uploads/online-privacy-bill-regulation-impact-statement.pdf (accessed 26/11/2021).

Bielefeld, S., Harb, J., & Henne, K. (2021). Financialization and Welfare Surveillance: Regulating the Poor in Technological Times. Surveillance & Society, 19 (3), 299-316.

Lowitja Institute. (2021). Close the gap: Leadership and legacy through crisis: Keeping our mob safe. Available from: https://humanrights.gov.au/our-work/aboriginal-and-torres-strait-islander-social-justice/publications/close-gap-2021 (accessed 26/11/2021).

New South Wales Government, Education Standards Authority. (2021). Digital technologies and ICT resources. Available from: https://educationstandards.nsw.edu.au/wps/portal/nesa/k-10/learning-areas/technologies/coding-across-the-curriculum (accessed 26/11/2021).

Thomas, J, Barraket, J, Wilson, CK, Holcombe-James, I, Kennedy, J, Rennie, E, Ewing, S, MacDonald, T. (2020). Measuring Australia's Digital Divide: The Australian Digital Inclusion Index 2020. RMIT and Swinburne University of Technology, Melbourne, for Telstra. Available from: https://apo.org.au/sites/default/files/resource-files/2020-10/apo-nid308474.pdf (accessed 26/11/2021).

Victorian Curriculum and Assessment Authority. (2021). Digital Technologies - rationale and aims. Available from: https://victoriancurriculum.vcaa.vic.edu.au/technologies/digital-technologies/introduction/rationale-and-aims (accessed 26/11/2021).