THE UNIVERSITY OF SYDNEY

Online Privacy Bill

Exposure Draft - Submission to the Attorney General's Department

Department of Media and Communications,
University of Sydney

6 December 2021

About the Department of Media and Communication at the University of Sydney

The Department of Media and Communications (MECO) is a world ranking group of scholars that continue to generate scholarship on the presence, evolution and impacts of digital media and its technologies on our societies and everyday lives. MECO focuses on the critical power of the humanities on all forms of media to investigate the rapidly emerging technologies and contemporary content practices. Our research areas are most obvious in digital cultures, social media, virtual realities, regulation and policymaking, journalism, platform governance and health communications. Some of our teaching areas include news and feature journalism, audio and video production, digital cultures, media theory and ethics, social media, public relations and health communications.

Our wide-ranging research and spirit of enquiry leads us to collaborate across the University, and indeed the world, in research partnerships targeting complex issues. We have a particular focus on digital media and digital cultures scholarship, which includes platform governance, human-computer interaction, and contexts and practices surrounding the use of digital technologies in households.

The content in this submission is the preliminary observations from the recently funded eSafety Commission Online Safety Research Grant scheme for the project *Emerging online safety issues: co-creating social media education with young people*.

Submission prepared by:

- Dr Jonathon Hutchinson, Senior Lecturer, Department of Media and Communications
- Dr Justine Humphry, Senior Lecturer, Department of Media and Communications
- Dr Olga Boichak, Lecturer, Department of Communications

Contact
Dr Jonathon Hutchinson
jonathon.hutchinson@sydney.edu.au
Phone: 0421 178 971

Executive Summary

The Online Privacy Code Privacy Legislation Amendment (Enhancing Online Privacy and Other Measures) Bill 2021 (henceforth referred to as the OP Code) seeks to address the increasing privacy concerns as a result of social media and other online media activities.

The OP Code will bind three key stakeholders groups to its regulatory measures:

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

While addressing the issues presented by the increased potential harm of date exposure due to digital communications, the OP Code has a particular focus on vulnerable groups such as older Australians, younger Australians, those with English as a second language, marginalised groups and those with disabilities. It aims to address the privacy practices of online platforms that can be detrimental to children and vulnerable persons, including sharing data for advertising purposes, or engaging in harmful tracking, profiling, or targeted marketing.

This submission refers to the Online Privacy Bill Exposure Draft, where the OP Code has identified children as one of the key vulnerable groups especially concerned with social media services. The three scholars named in the submission have recently secured a funded research project with the eSafety Commissioner to explore further the key issues identified in this document. Within the next 12 to 18 months, the research data from this project will be available to clearly articulate the emerging issues for young Australians and their parents or carers who engage with social media. The project is a co-designed approach to place the voice of young Australians and their parents/carers at the centre of the findings while prioritising a shared responsibility for their online safety. Two members of the project research team also attended the Attorney-General Department's Consultation - Privacy Protections for Children held on the 19th November, 2021.

To that end, this submission will focus on the following eight key areas of concern that have already been identified for further investigation and research, where the same areas of concern are also present within the OP Code:

1. *Technologically enabling consent*

Consent has emerged as a key issue for young people and their parents and carers, with the OP Code introducing stricter requirements for social media companies and other 'electronic services' in the handling of personal information and new responsibilities of consent for parents and guardians. At this stage it is unclear how these requirements in the Code in relation to obtaining consent, age verification or verification of consent, will be technologically implemented and monitored to ensure young people are adequately supported through their social and online media experiences.

2. *Retroactive age verification and consent*

In many cases, young Australians are already using a range of social and online media services often with prior parental or carer consent. In these cases, and as the OP Code comes into operation, how will it be applied retrospectively? How will the problem of 'consent fatigue' and the impracticalities of obtaining verifiable parental or guardian consent retrospectively be managed?

3. *Recognising age range capacity differences and disability differences*

The Code has gone so far as to identify two demarcations of age groups for young Australians: 12-16 and 16-18. However, there is an incredibly varying range of maturity and mental capacity within these age groups which impacts on an individual's ability to consent to

variations, actions and exemptions. This concern extends to those users living with disabilities or with cognitive impairment.

4. User voice

While the consultation is open to a wide range of interested stakeholders for the increased safety and protection of Australian social and online media services, it has become obvious the user voice (young Australians) is missing from the discussion. In addition to this, the voice of parents, guardians or representatives of those young people is also not obvious. We would ask the Attorney General's Department to not engage with industry consultation in the first instance, but to instead consult extensively with those who will be impacted most by these legislative changes.

5. Legitimate exemptions for independent consent

It is clear there are a number of scenarios where parental and carer consent is not appropriate for young users of social and online media services. In these instances, how will young people be able to exercise independent consent for their own health, safety and well-being? What mechanisms will be put in place to support children under the age of 16 to provide independent consent to collection for situations where they have capacity, and how will this capacity be determined?

6. Cultural difference and varied parenting arrangements

In many instances of the OP Code, the perspective is assumed to be from one of an imagined family and their use of social and online media services. This will not be the case in many applications of the Code where a variety of cultural, religious, ethnic and gendered backgrounds are present. The application of consent for the services within the OP Code will likely be different for these groups in contrast to what is currently the demonstrated application in the Exposure Draft, and will involve different contexts and requirements for obtaining consent and negotiating requirements of age verification.

7. Digital literacy among parents and children

The capacity to interpret and implement these changes of the OP Code will for the most part be left to that of the parents and guardians of young Australians. There is an assumption that these individuals embody the capacity to both understand the Code and the digital ability to implement the relevant technological processes for consent. As the Australian Digital Inclusion Index (Thomas et al., 2021) has shown, the digital ability of Australians (which includes values and attitudes toward technology use) remains an issue. Compounding the implementation of the Code on to those who care for young Australians is not an ideal scenario that the Attorney General's Department should be pursuing.

8. Definition of 'electronic service'

The OP code will apply to organisations that provide an electronic service defined as hardware, software, websites, mobile applications, hosting services, peer-to-peer sharing platforms, instant messaging, email, SMS and MMS, chat services, and online gaming. It is unclear whether this definition of an 'electronic service' encompasses online education platforms and health apps and services, such as smart watches and other wearables as well as a wide range of IoT based platforms such as smart voice assistants and smart toys and robotics, which are regularly used by children and have an online component and/or collect data through voice, touch or facial recognition.

Scope of the OP Code

The Impact Statement of the OP Code outlines several areas where the Code will have repercussions for those providing social and online media services. Those provisions present an additional number of implications for those who use those same services. In pre-empting the areas of impact that may be generated by the OP Code, The Attorney General has highlighted some of the areas to focus our research toward, while also providing a number of potential and existing areas of conflict for younger social media and online media users. These are useful areas to highlight for further discussion particularly for a variety of stakeholders voices, including young people and their parents and guardians or representatives.

The following three impact areas are especially important to the younger users of social and online media services. Expanding on the Executive Summary, we have identified several implications that align with the impact of the provisions of the OP Code that the Attorney General needs to further consider as the consultation process and development of the Code proceeds.

The team from the Department of Media and Communications at the University of Sydney who contributed to this submission are currently conducting research in this space. It is worth highlighting that the very trajectory of the developing OP Code aligns with the research currently underway. As part of this eSafety Commissioner funded research project – *Emerging online safety issues: co-creating social media education with young people* – the research team are exploring a number of areas that impact on young people's use of social media. Specifically, we are working with culturally and linguistically diverse (CALD) groups, young Indigenous users, and other marginalised groups located in regional and metropolitan New South Wales who frequently use social media, and who are aged between 12 years and 18 years old. Over this research project, the team will investigate safety issues focusing on emerging areas of online harm from the perspective of young people and their carers.

The research data will be collected and analysed in 2022/23, and we are willing to engage in further discussions around the results with the Attorney General at that time. However, at this stage we are able to offer some preliminary insights from our research to date which align with the current discussions underway for the OP Code and will help guide further insights as the Code is developed.

Impact: Take all reasonable steps to verify the age of individuals who use the social media service

Impact Statement 1: Technologically enabling consent

Consent has emerged as a key issue for young people and their parents and guardians, with the Code introducing stricter requirements for social media companies in the handling of personal information and new responsibilities of consent and age verification for children under the age of 16. At this stage it is unclear how requirements in the Code in relation to consent, age verification or verification of consent, will be technologically implemented and monitored to ensure children and young people are adequately supported through their social and online media experiences.

The current systems and processes that are in place for social media platforms to obtain permission from users for data collection are complex and require specialist expertise to enable seamless integration. From initial account registration, through to enabling comments to appear from a Facebook signed-in state on a blog or website, or connecting a personal tracking device to a social media platform, there exist a wide range of systems and processes that platforms use to connect and communicate with each other and to obtain upfront consent and ongoing permission for changes in what or how user data is collected.

It is likely that technical systems will be developed and used by platform companies to implement new consent requirements but it is currently unclear what these will be and how they will be technologically-enabled, what proof of age will be required and how consent will be verified. At present, these processes are often enabled at the user side through the account registration stage but there are also ongoing requirements for consent or permission resulting from changes in data collection, services or the age and/or capacity of the user.

At present, these ongoing processes are often enabled at the user side with a permission request, for example to allow a website to access a user's Facebook account which will in turn enable the user to comment on the website from a signed-in state on Facebook. While this has become common practice for users to 'accept' the permission request, there is uncertainty around the process in terms of what permission is being provided, and how the process operates for users. Further to this, permission does not equal consent in the context of the OP Code, raising questions about whether these changes in data collection at different points of use will be covered by consent provided by parents or guardians after account registration. While it is relevant to consider how to avoid 'consent fatigue' around such data collection changes, it also raises the issue of whether 'permission requests' might be used to avoid or get around consent requirements and how to evaluate whether a change in data collection is substantial enough to warrant the need to re-seek consent.

Impact Statement 2: Retroactive age verification and consent

The digital media environment of which the OP Code seeks to address is a complex combination of social media and other digital platforms operating interchangeably. In many cases, young Australians are already using a range of social and online media services often with prior parental or carer consent. In these cases, and as the OP Code comes into operation, how will it be applied retrospectively? How will the problem of 'consent fatigue' and the impracticalities of obtaining verifiable parental or guardian consent retrospectively be managed?

Consent fatigue becomes a crucial item under the consideration of the Code's implementation. As a result of the General Data Protection Regulation (GDPR) in the European context, internet users are required to accept various conditions when they visit a website for the first time. Often these conditions are for harmless 'cookies' that enable certain technologies to operate, or they could be for conditions and permissions that are considerably more elaborate and

complex. In either case, user fatigue is a common practice where users will simply 'Accept All Conditions' in order to access the website. This scenario is also familiar to the sign-up process for social media accounts, where users are presented with tens or hundreds of pages of overly and unnecessarily complicated Terms of Services that a new user is expected to read, understand and agree to prior to using the service. User fatigue has become a significant issue in both of these scenarios, and one that is also a potential for the implementation of the Code.

The concept of age calibration across these varied digital platforms is also not consistent and could be further complicated through retrospective age verification. For example, a younger user who is 10 years old might wish to play a seemingly harmless game online which is rated for audiences 8 years old and above, yet they require a Facebook account to login to and access that platform. Gaming is one example where age calibration for younger users has presented complex consent issues for parents and carers to make often ill-informed decisions. Nevertheless, many under-age users have access to these services for a broad spectrum of purpose for reasons that may extend beyond simply having an Instagram or TikTok account.

Impact: Ensure the collection, use or disclosure of a child's personal information is fair and reasonable in the circumstances, with the best interests of the child being the primary consideration when determining what is fair and reasonable

Impact Statement 3: Recognising age range capacity differences and disability differences

The Code has gone so far as to identify two demarcations of age groups for young Australians: 12-16 and 16-18. However, there is an incredibly varying range of maturity and mental capacity within these age groups which impacts on an individual's ability to consent to variations, actions and exemptions. This concern extends to those users with disabilities and cognitive impairment. References to 'fair and reasonable use' and 'the best interests of the child' are important for placing the onus on social media platform companies to limit the collection, use or disclosure of a child's personal information to only certain reasons that are well-justified. However, how these terms will be interpreted and implemented are unclear, and would similarly vary depending on age and maturity.

We suggest the Attorney General invest considerably into constructing a typology that is broader and more generative for mental and maturity capacities of individuals beyond age alone. While it is useful to think about users in age group demarcations, it does not accurately reflect the users themselves, especially for younger users who seek legitimate exception from consent for these services (see Impact Statement 5 rationale below).

Social media platforms especially are commercial operations often with shareholders that require these companies to make profit as a return on investing with them. That is to say that commercial social media providers, while enabling unprecedented connection and communication possibilities, are not providing a public service. Thus while integrating a more graded typology of mental and maturity capacities and age-appropriate definitions of 'best interests' can support a more relevant approach to data collection, consideration must be given to whether industry is in a position to lead its implementation and make sound interpretations in the context of being led by market-driven interests in a data-brokering industry where the data generated by social media use has become a product of itself, to be traded as a commodity, monetised and exchanged between organisations (Speikermann, 2019).

Impact Statement 4: User voice

While the consultation is open to a wide range of interested stakeholders for the increased safety and protection of Australian social and online media services, it has become obvious the user voice (young Australians) is missing from the discussion. In addition to this, the voice of parents and carers of those young people is also not obvious. We would ask the Attorney General's Department to not engage with industry consultation in the first instance, but to instead consult extensively with those who will be impacted most by these legislative changes and to provide the opportunity for user-led development of the OP Code. We see this as an opportunity for Australia to pioneer a user-centred Code development process, recognising that the Code needs to work for users of social media and other electronic services as much as for Industry.

In doing so, re-ordering the consultation and OP Code development process to give priority to young people and their parents and guardians: in the first instance it acknowledges that these significant changes to their digital lives are underway, second it provides an opportunity to understand the proposed changes within the Code and its implications, and third, it includes

their voice as a considerable stakeholder group of concern for this legislation. Our preliminary research has indicated that this group especially are unaware of the changes afoot and are confused and overwhelmed by the process and the potential implications of the Code. Bringing children and young people as well as their parents or guardians into the OP Code development process will have the positive effects of increasing digital literacy and skills in the regulatory mechanisms and processes that they need to understand and take part within.

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

Impact Statement 5: Legitimate exemptions for independent consent

It is clear there are a number of scenarios where parental and carer consent is not appropriate for young users of social and online media services. For example, girls seeking health information about menstruation or LGBTIQ youth who want to connect with like minded peers as they explore their sexuality. There are situations and environments that are not conducive to children and young people having to obtain consent from their parents or guardians, for example, children in institutional care, detention or in a violent domestic environment. In these instances, how will young people be able to obtain consent or seek legitimate exemption from consent for their own health, safety and well-being? There needs to be defined parameters for legitimate exemptions from consent and an easy-to understand and use mechanism for children to be able to exercise independent consent in these and other legitimate circumstances.

Further to these kinds of specific cases or circumstances, there is the wider concern that introducing a consent system that is overly restrictive will lead to exclusion from digital services. There is broad agreement that children and young people's ability to participate in social media is essential for identity formation, building friendships and peer-groups, for developing skills and connections and for leisure and entertainment (Livingstone, Mascheroni, & Staksrud, 2017; Milosevic, 2017). While the research team making this submission strongly support the development of a binding code of practice for social media and other online platforms that trade in personal information, there is a real risk that an overly restrictive consent and age verification system will reduce young people's independence and introduce new kinds of harms in the form of being excluded from services that they rely on. The urge to protect children from real and perceived dangers can inadvertently lead to the over-reliance on 'gatekeeping through consent' shifting the onus away from cultivating children and young people's independence and digital skills and developing a less abusive social media environment.

Impact Statement 6: Cultural difference and varied parenting arrangements

In many instances of the OP Code, the perspective is assumed to be from one of an imagined family and their use of social and online media services. This will not be the case in many applications of the Code where consent is being sought and negotiated for these services in households and family contexts composed of a variety of cultural, linguistic, religious, ethnic and gendered backgrounds, with family practices and relationships that are likely to be different to that which is currently demonstrated and assumed in the Exposure Draft. Households that have extended and/or multi-generational family members living under the

same roof, different languages spoken and shared parenting arrangements are just some examples of household compositions and contexts in which responsibilities of consent may be shared within and/or across households and even states or countries.

Impact Statement 7: Digital literacy among parents and children

The capacity to interpret and implement these changes of the OP Code will for the most part be left to that of the parents and carers of young Australians. There is an assumption that these individuals embody the capacity to both understand the Code and the digital ability to implement the relevant technological processes for consent. As the Australian Digital Inclusion Index (2021) has shown, digital ability of Australians remains an issue, and any new privacy protections and consent requirements that are at least in part technologically-enabled will generate additional skills and literacies needed to navigate this new legal and digital environment. Compounding the implementation of the Code on to those who care for young Australians is not an ideal scenario the Attorney General's Department should be pursuing.

Further impacts:

Impact Statement 8: Definition of 'electronic service'

The OP code will apply to organisations that provide an electronic service defined as hardware, software, websites, mobile applications, hosting services, peer-to-peer sharing platforms, instant messaging, email, SMS and MMS, chat services, and online gaming. While the broadening of the definition of 'electronic service' is an important addition to the new bill, there are a number of existing and emerging technologies that are regularly used by children and have an online component and/or collect data that are not specifically covered in the existing breakdown/table encompassing the different types of electronic services. For example, smart watches and other wearables as well as a wide range of IoT based platforms such as smart voice assistants and smart toys and robotics, which collect data through a wide variety of sensing technologies including voice, touch or facial recognition are not explicitly listed. We note that IoT and smart technologies have been identified as areas in need for stronger privacy protections around data collection and also point out that these technologies provide quite different interaction environments to social media sites that are not necessarily conducive to the same consent and age verification processes. To account for emerging sensor-driven electronic services that involve data collection we suggest a review of the definition of 'electronic services' and how new provisions of privacy around data collection would apply to these technologies and industries.

References

Livingstone, S., G. Mascheroni, and E. Staksrud. (2017). European research on children's internet use: Assessing the past, anticipating the future. New Media & Society January 10:1–20.

Milosevic, T. (2018). *Protecting children online?: Cyberbullying policies of social media companies*. Massachusetts: The MIT Press.

Speikermann, M. (2019). Data Marketplaces: Trends and Monetisation of Data Goods. *Intereconomics, 2019*(4), 208–216.

Thomas, J., Barraket, J., Wilson, C. K., Rennie, E., Ewing, S., & MacDonald, T. (2021). *Measuring Australia's Digital Divide: The Australian Digital Inclusion Index 2021*.

Contact

Faculty of Arts and Social Science, School of Literature, Arts and Media, Department of Media and Communications

Level 2
John Woolley Building (A20)
Manning Road, Camperdown NSW 2006

Phone: 02 9351 2821

jonathon.hutchinson@sydney.edu.au
justine.humphry@sydney.edu.au
olga.boichak@sydney.edu.au

sydney.edu.au

CRICOS 00026A

THE UNIVERSITY OF
SYDNEY