Submission to the Online Safety Charter consultation, April 2019

5 April 2019

To: Director, Online Content and eSafety Section
Department of Communications and the Arts
onlinesafety@communications.gov.au

Submitted by:
Associate Professor Michael Salter
Scientia Fellow, Criminology
School of Social Sciences
University of New South Wales

Dr Noam Peleg
Lecture, Faculty of Law
University of New South Wales

Re: Submission to the Online Safety Charter consultation

Thank you for the opportunity to contribute to the Online Safety Charter consultation. Our comments below draw on our respective areas of research and expertise, including child sexual exploitation, child safety and technologically-facilitated abuse (Salter) and international children's rights law and family law (Peleg). A/Prof Salter's research focuses on organised forms of child sexual abuse and the role of technology in child abuse, domestic violence and sexual assault. He is the author of *Organised Sexual Abuse* (2013) and *Crime, Justice and Social Media* (2017) and he sits on the Board of Directors of the International Society for the Study of Trauma and Dissociation. He was an expert advisor to the Royal Commission on Institutional Responses to Child Sexual Abuse and he is currently leading national studies into multi-sectorial responses to complex trauma, and the role of parents in the creation of child exploitation material (CEM), funded by the Australian Centre to Counter Child Exploitation. Dr Peleg research focuses on international children's rights law, and the right to development of children. He is a member of the academic board of the International Journal of Children's Rights and has consulted the UN Committee on the Rights of the Child.

Discussion question: Who should be responsible for ensuring built-in child safety?

> *The Australian government should impose a statutory "duty of care" on technology companies to ensure online child safety and protection, encompassing content regulation and safety by design principles, to be enforced by the eSafety Commissioner. Social media companies and internet service providers should be*

required to abide by the National Principles for Child Safe Organisations drawn from the work of the Royal Commission into Institutional Responses to Child Sexual Abuse and endorsed by the Council of Australian Governments.

This submission is focused on child safety on social media and other internet services that generate revenue based on user interaction and uploaded content. We assert that companies whose business model and online architecture includes the likely engagement of children below the age of 18 in online interactions with adult strangers have a heightened responsibility to those children. We also assert that internet services whose platform design is presently facilitating interaction *between* adults with sexual interests in minors, and the exchange of CEM, are causing direct harm to children, and causing social harm through the development of abuse networks and the dissemination of discourses and subcultures that normalise the abuse of children. Child sexual abusers have proven adept at identifying and exploiting the opportunities afforded by social media to interact with children and each other, while internet services have consistently failed to proactively identify and address these problems.

While we recognise the role of multiple stakeholders in the promotion of child safety and wellbeing, online and offline, industry is responsible for ensuring that the services and products they bring to market are safe for its users, especially children. As our submission will demonstrate, industry self-regulation and co-regulation has been insufficient to ensure the safety of children online. Therefore, and in the wake of escalating reports of online child exploitation and paedophile activity on social media, our submission recommends the replacement of industry self-regulation and co-regulation frameworks, which experience prove to be ineffective, with legislation that establishes a clear and enforceable duty of care to children on social networks. The current implementation of the National Principles for Child Safety Organisations provides an important opportunity to integrate technology industries into the national broader child protection framework, to ensure that the lessons of the recent Royal Commission into Institutional Responses to Child Sexual Abuse are applied to online as well as offline environments.

Australian government obligations for child safety

Under international treaties, the Australian government has an obligation to ensure the protection of children in all areas of life, including online. Any regulation of children's online safety should take into account Australia's obligations and duties under the UN Convention on the Rights of the Child (CRC), which Australia signed and ratified in 1990. First and foremost, any form of regulation should consider the Convention's four guiding principles: the right to non discrimination (Article 2); the principle of the best interests of the child (Article 3); the right to life, survival and development (Article 6); and the right to participation of children (Article 12).

Article 3 is a threefold concept (CRC/C/GC/14 2013, par 6). First, as a substantive right of the child, the child has a right to have her best interests assessed and taken as a *primary* consideration in order to reach a decision on the issue at stake. Designing a framework that has such an immense effect of children's direct and indirect engagement with the digital space, as the consultation paper suggests, must explicitly account for children's best interests. Second, the principle of the child's best interests, while not the only consideration, should be prioritized over other considerations. In the context of this consultation process,

when making a recommendation or designing a framework for prevention and when more than one course of action is available (for example, respond time by industry's monitoring body, self-regulation or external regulation), than the decision that most effectively serves the child's best interests, and does not conflict with other provisions of the Convention, should be preferred. Third, the best interests principle is a procedural rule: any decision-making process should include an evaluation of the possible impacts (positive and negative alike) of the decision on the child or children concerned. The justification for making a specific decision or recommendation should demonstrate how the best interests principle has been taken into account, including what criteria it is based on and how the child's interests have been weighed against other considerations. In other words, assumption about what might be best for children should not be made in the abstract, but rather must be made based on evidence and, where available, empirical knowledge. When such knowledge is not available, more research should be conducted.

The second right that should be considered is children's right to participate in decisions concerning their life (Article 12 CRC). This means, in the context of this consultation process, that children themselves should have the opportunity to express their views, concerns, experiences and recommendation about the content of any future guidelines, and to provide specific comments about the suggested framework. Currently, we didn't see any evidence that children, either directly or indirectly, were part of the process, although we understand that the Office of the eSafety Commissioner undertook consultation with young people as part of the development of their "safety by design" recommendations. However, the Australian government has a duty to enable children to exercise their right to participation in this consultation process on a matter of central importance to their safety.

Other two core elements of the CRC that require attention is the right of children to non discrimination (Article 2 CRC), and their rights to life, survival and development (Article 6 CRC). As for the right to non discrimination, it is submitted that any information provided for children, including, for example, the "report buttons" that the consultation paper considers, or any other information displayed online (or provided for children in schools, community centres and other location, flagging out the opportunities and danger that the online environment presents), should be made available for children not only in English but also in other languages commonly spoken in Australia, and be made accessible for children with hearing or visual disabilities. Last, and while there is an urgent need to protect children in the online space, any future framework should also account to the fact that the online space is also an opportunity for development, including intellectual and educational development, social development (and social interaction), and moral developmental. As such, any restrictions or limitation should ensure that children's opportunities to engage, to learn and to interact are not compromised due to the need to protect them from abusive adults (or other children).

Other rights of children that should be taken into account in the designing process are the right to education, which includes the right to child's personality, talents and mental and physical abilities to their fullest potential (Articles 28-29 CRC), the right to bodily integrity and protection from abuse (Article 19 CRC), and the right to information (Article 17 CRC). We would like to emphasise that the realisation of the latter also includes an explicit duty to develop "…appropriate guidelines for the protection of the child from information and material injurious to his or her well-being, bearing in mind the provisions of articles 13 and 18." (Article 17(4)).

There are a range of ways in which Australia can execute its duties towards children. Some of the ways in which it does so in other contexts can be useful models in our context. For example, the regulation of the sale of alcohol. Current legislation frameworks not only set the minimum legal drinking age but also create a web of licencing regulatory framework for the sale of alcohol in bottle shops, pubs and hotels. These laws, which vary from state to state, essentially requires private owners to invest time, money and effort to ensure that no one below the age of 18 will purchase or consume alcoholic drinks. The laws, by in large, also holds these private, for-profit, entities to account, and suggest that violation of this duty, which can be describe as a duty of care, will result in a fine and other, more intrusive, measures. In this space, argument concerning the added cost that these duties create, that it is unrealistic to expect each bartender or sales person to verify the identity and age of each customer, or that regulation should not be introduced as the industry can regulate itself and ensure that no one under age will be served alcohol, have been rejected. Similarly, these sorts of arguments should be rejected in the context of this consultation process too. The magnitude of the social problem and the risk that children are facing, and the proven ineffectiveness of industry self-regulation, suggest that a robust, comprehensive and enforceable regulation should be introduced.

Government regulation of online safety

While online safety regimes in Australia have focused on the regulation of content, internet service providers and social media platforms are not merely publishers of content but rather they facilitate and structure interaction and communication through their platform design and administration (Salter, 2017). The manner in which platforms facilitate interaction between users shapes the level of risk to users on a given platform (Salter, 2018). However, as technology companies develop their products, child protection has not been a priority and hence there are now a range of online products with design flaws and administrative regimes that predictably expose children to harm and abuse. An over-reliance on inexpensive algorithmic and automated safety measures and insufficient investment in proactive human moderation has created numerous safety loopholes for the abuse of children, and in some cases, resulted in technology industries inadvertently earning income from online paedophile activity. Attempts to retroactively address these harms have proven to be insufficient. There are numerous recent examples in online child exploitation activity on social media has been exposed through the proactive investigation of journalists and social media users rather than by the platform itself, which is then often forced into a post hoc response to negative publicity.

- **WhatsApp:** WhatsApp is the most popular message application with over one and a half billion users. In December 2018, the Israeli non-government organisations Screen Savers and Netivei Reshet published a report documenting the use of WhatsApp chat groups to share CEM (Constine, 2018b). Third party apps for identifying WhatsApp groups, available for download via Google Play, enabled users to identify active rings of users trading in CEM. The names of some of these groups included specific references to CEM, and so their nature and content should have been obvious to WhatsApp moderators. Furthermore, third party apps for discovering WhatsApp CEM groups were running Google and Facebook's advertising networks, enabling the apps to monetize their activities while generating income for technology companies. In the wake of media publicity, Google Play removed identified third party

apps that facilitated CEM exchange on WhatsApp, and Google and Facebook blocked these apps from their ad networks (Constine, 2018a).

- **YouTube:** In February 2019, YouTube user Matt Watson uploaded a viral video to YouTube exposing the prevalence of networks of paedophiles and sexualised videos of children on YouTube.[1] Watson documented the way in which the YouTube algorithm was, through its "recommend" system, linking together a large number of self-created video content of young children and teenagers engaged in activites such as dancing, doing gymnastics and swimming. Once a user has watched a couple of these videos, the YouTube "recommend" system automatically provides the user with playlists of similar content, creating what Watson identified as an algorithmically generated CEM network on YouTube. Some of these videos include moments where the child inadvertently or intentionally exposes body parts or engages in other forms of bodily display. These videos have attracted a high number of views and comments from paedophiles, who have used the "comment" function of YouTube to provide timestamps for parts of the videos where the child may inadvertently expose body parts, links to other provocative YouTube videos of children, or exchanging contact details with one another. These videos have been monetised by YouTube, including pre-roll and banner advertisements (Orphanides, 2019).
- **TikTok:** TikTok is an app that enables users to post videos of themselves lip synching and dancing to popular songs. The app has a strong user base amongst children. Journalists have identified an active community of TikTok users who appear to be soliciting nude images from children while minor users are complaining about repeated solicitation for sexualised images (Cox, 2018). Some TikTok user profiles include open statements of interest in nude images and the exchange of sexual videos, including invitations to trade material via other apps. Concern about paedophile activity on TikTok have led some users to begin identifying concerning user activity and circulating user names of men who are alleged to be contacting and interacting inappropriately with children on the site. The fact that TikTok users are resorting to the self-policing of paedophile activity on the platform raises concerns about the level of proactive regulation and monitoring of users who seek to engage in the sexual exploitation of children.

The focus on the regulation of online content within existing online safety legislation, frameworks and industry codes of practice have proven to be insufficient to address the effects of platform architecture, administration and automated/algorithmic functions on child safety. Co-regulation approaches have evidently failed to ensure the industry prioritisation of child safety. As outlined below, there is increasing international consensus that responsibility for online child protection cannot, and should not, be devolved to industry or the community, but rather the role of government should be to set enforceable benchmarks for online child safety. To be effective, these benchmarks should expand beyond the focus on content regulation that has dominated the Australian approach to online safety to date, to address the role of product design in creating safe or unsafe online environments for children.

[1] The video is available at https://www.youtube.com/watch?v=O13G5A5w5P0. At the time of writing, it has been viewed over three and a half million times.

In the United Kingdom, there is significant support for a statutory duty of care to be imposed on social media and technology companies. The House of Lords Select Committee on Communication recently released a report on online regulation, which concluded that industry self-regulation has failed to ensure the safety of the public, and called specifically for the imposition of a legislative "duty of care" on social media platforms (House of Lords, 2019). They recommended ten principles to guide the development of online safety, including that "the same level of protection must be provided online as offline", that services must be designed to "act in the interests of users and society", and the prioritisation of child safety. Ongoing harms to children on social media and the unreliable and inconsistent responses of industry have prompted the National Society for the Prevention of Cruelty to Children in the UK to advocate for strong and independent statutory regulation of social media in which platforms are subject to a legally enforceable duty of care (NSPCC, 2019).

In Australia, the recent Briggs (2018) review also noted the failure of industry co-regulation to ensure the safety of internet users and argued for a new industry code that is mandatory with penalties for non-compliance. This code would include key "safety by design" principles enforced by the eSafety Commissioner to ensure that the online products bought to market – and particularly those advertised to, and taken up, by minors – are safe and have been designed to inhibit misuse, abuse and exploitation (Briggs 2018, p. 23). As Briggs noted, her findings are commensurate with the recent joint statement from Ministers from Australia, Canada, New Zealand, the UK and the USA calling on industry to prioritise "the protection of the user by building user safety into the design of all online platforms and services, including new technologies as they are deployed".[2] The existing research of the eSafety Commission on "safety by design" principles provides a robust evidence base for the development of an enforceable duty of core of internet service providers to users, encompassing content regulation but also platform design and administration.

An enforceable duty of care of internet service providers to children, informed by the National Principles of Child Safe Organisations

The National Principles were developed in response to the recommendations of the Royal Commission into Institutional Responses to Child Sexual Abuse, which found that many organisations had failed in their responsibilities to protect children from sexual abuse or to respond appropriately when notified of abuse. The National Principles aim to foster a nationally consistent approach to child safety and protection from sexual abuse across all sectors of Australian society, including technology and the internet. The National Principles are:

1. Child safety and wellbeing is embedded in organisational leadership, governance and culture.
2. Children and young people are informed about their rights, participate in decisions affecting them and are taken seriously.
3. Families and communities are informed and involved in promoting child safety and wellbeing.
4. Equity is upheld and diverse needs respected in policy and practice.

[2] https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/five-country-ministerial-2018

5. People working with children and young people are suitable and supported to reflect child safety and wellbeing values in practice.
6. Processes to respond to complaints and concerns are child focused.
7. Staff and volunteers are equipped with the knowledge, skills and awareness to keep children and young people safe through ongoing education and training.
8. Physical and online environments promote safety and wellbeing while minimising the opportunity for children and young people to be harmed.
9. Implementation of the national child safe principles is regularly reviewed and improved.
10. Policies and procedures document how the organisation is safe for children and young people.

Despite the fact that children constitute an important market and consumer base for the technology industry, it is apparent that social media platforms and internet service providers are not "child safe" organistions, defined as organisations that put the best interests of children and young people first. Therefore, social media and internet service providers should be required to abide by the National Principles and annually audited for compliance, alongside the thousands of other child-focused institutions in Australia who are now required to benchmark their child safety measures.

Bibliography

Briggs, L. (2018). *Report of the Statutory Review of the Enhancing Online Safety Act 2015 and the Review of Schedules 5 and 7 to the Broadcasting Services Act 1992 (Online Content Scheme).* Canberra: Commonwealth of Australia. At: https://www.communications.gov.au/file/47865/download?token=VsfBbUcY

Constine, J. (2018a, December 27). Google & Facebook fed ad dollars to child porn discovery apps. *Techcrunch. At:* https://techcrunch.com/2018/2012/2027/funding-filth/

Constine, J. (2018b, December 20). WhatsApp has an encrypted child porn problem. *Techcrunch.* At: https://techcrunch.com/2018/2012/2020/whatsapp-pornography/

Cox, J. (2018, December 6). TikTok, the app super popular with kids, has a nudes problem. *Motherboard.* At: https://motherboard.vice.com/en_us/article/j5zbmx/tiktok-the-app-super-popular-with-kids-has-a-nudes-problem?utm_source=mbtwitter

House of Lords. (2019). *Regulating In a Digital World*. Select Committee on Communications. 2nd Report of Session 2017–19. House of Lords. At: https://publications.parliament.uk/pa/ld201719/ldselect/ldcomuni/299/299.pdf

NSPCC. (2019). *Taming the Wild West Web: How to Regulate Social Networks and Keep Children Safe From Abuse*. London: NSPCC. At: https://www.nspcc.org.uk/globalassets/documents/news/taming-the-wild-west-web-regulate-social-networks.pdf

Orphanides, K. G. (2019, February 20). On YouTube, a network of paedophiles is hiding in plain site. *Wired.* At: https://www.wired.co.uk/article/youtube-pedophile-videos-advertising

Salter, M. (2013). *Organised Sexual Abuse*. London: Glasshouse/Routledge.

Salter, M. (2017). *Crime, Justice and Social Media*. London and New York: Routledge.

Salter, M. (2018). From geek masculinity to Gamergate: the technological rationality of online abuse. *Crime, Media, Culture, 14*(2), 247-264.