**Privacy and children’s rights: Considering the role of non-state actors in the dissemination of a child’s personal information online**

*Cassandra Seery[[1]](#footnote-1)*

*A submission to the Committee on the Rights of the Child regarding the proposed General Comment on children’s rights in relation to the digital environment*

1. Introduction
2. When the *Convention on the Rights of the Child* came into force in 2 September 1990, there was no meaningful way to consider the impact of the digital environment on children. The invention of the World Wide Web – the internet as we know it today – effectively began entering the mainstream population from 1990, and it was not until the launch of social media applications from the early-2000s that significant privacy questions began to emerge. As we reach 2020, it has become clear that children’s rights under the CRC are not only applicable to the digital environment, but that the digital environment is having an increasing impact on children’s rights outside the digital space.
3. While there has been an increasing focus to better equip children with the tools and skills to interact with a digital environment safely,[[2]](#footnote-2) there has been almost no discussion about the impact of duty bearers (such as parents, caregivers and others) sharing personal information about children in a digital environment and the impact this may have on children’s rights. Additionally, there has been no meaningful discussion concerning the role of the State and relevant corporations (as non-state actors) in regulating the digital environment in relation to children’s rights.
4. The proposed General Comment presents an opportunity to: (i) clarify the relationship between a parent’s right (as an individual) and their obligations as a parent to ensure the safety and privacy of their children online; and (ii) provide guidance to States on how to approach Convention obligations in a digital environment in relation to the conduct of non-state actors[[3]](#footnote-3). This submission seeks to briefly raise some key issues associated with dissemination of a child’s personal information by third parties and possible opportunities to provide guidance to States on mechanisms to address this with third parties (both individuals and organisations).
5. Dissemination of children’s personal information by non-state actors

***Problematic Behaviours***

1. The dissemination of a child’s personal information online can take a number of forms. These disclosures are traditionally made by parents who share personal information about their children through applications such as Facebook, Instagram, Snapchat and other similar social media platforms. A 2018 study undertaken by the London School of Economics found that three in four parents regularly posted photos and videos of their children on social media and other platforms.[[4]](#footnote-4) These disclosures are generally considered legal domestically[[5]](#footnote-5) and children have no positive rights to prevent such disclosures. Indeed, their status as a minor ensures that their ‘rights’ are entrusted to parents[[6]](#footnote-6) who are presumed to be acting in a child’s best interests; as a consequence they are entrusted with a child’s personal information and control the circumstances in which that information is released.
2. In a pre-digital environment, the dissemination of a child’s personal information was generally limited to individuals directly connected to the child and the State. The evolution of the digital environment, in particular the rise of social media, now allows third parties to disseminate a child’s personal information in an instantaneous and unregulated environment.[[7]](#footnote-7)
3. Currently, problematic behaviours by third parties that interfere with children’s rights can be categorised by two behaviours:
   1. Sharing images (photos, videos and live streams) of children online, particularly via social media platforms.
   2. Sharing identifying details of children online. This includes: the full name of the child and the date and time of birth. When combined with geographical information, this can also include: where a child lives (by suburb, region or country), where they attend school, their friendship networks, and the nature and location of their extra-curricular activities.
4. These problematic disclosures are further exacerbated by a number of factors:
5. Any content[[8]](#footnote-8) that is uploaded to social media platforms give those businesses an immediate, unfettered licence to distribute without being sued. For example, Facebook’s *Terms of Service* states:

*‘To provide our services…we need you to give us some legal permissions to use this content. Specifically, when you share, post or upload content that is covered by intellectual property rights (e.g. photos or videos) on or in connection with our Products,* ***you grant us a non-exclusive, transferable, sub-licensable, royalty-free and worldwide licence to host, use, distribute, modify, run, copy, publicly perform or display, translate and create derivative works of your content*** *(consistent with your privacy and application settings). This means, for example, that if you share a photo on Facebook,* ***you give us permission to store, copy and share it with others*** *(again, consistent with your settings) such as service providers that support our service or other Facebook Products that you use. You can end this licence at any time by deleting your content or account’*(emphasis added).[[9]](#footnote-9)

It should be noted that while the *copyright* of the photo remains with the owner of the content, the global dissemination of content on these platforms makes the control of distribution impossible and arguably negates the ownership of the material to a significant degree. This is best exemplified by terms such as the one below, which assert that terminating a licence does not guarantee that information will no longer be shared:

*‘You should know that, for technical reasons,* ***any content that you delete may persist for a limited period of time in backup copies*** *(though it will not be visible to other users). In addition,* ***content that you delete may continue to appear if you have shared it with others and they have not deleted it’*** (emphasis added).***[[10]](#footnote-10)***

1. Uploading and sharing content online is an instantaneous process with no checks or warnings before it is disseminated. The facility to include such proactive protections is available,[[11]](#footnote-11) however they are not being utilised to prompt users to confirm that the information they share about children is being done safely and legally.
2. Social media companies are proactive in what is known as non-user data collection, which results in companies such as Facebook developing ‘shadow profiles’ of non-users (including children) without the consent of either the child or the parent.[[12]](#footnote-12) It should also be noted that non-users – and parents of non-users - do not have any direct control over shadow profiles. These profiles are created by the information gathered from third party users (including parents) and any personal information can be added to a child’s shadow profile. Additionally, tech companies have arguably been implementing other measures[[13]](#footnote-13) that are designed to exploit users[[14]](#footnote-14) rather than protect them. This can indirectly impact on children where their information is being disseminated by third parties.
3. Parents, caregivers and other individuals have varying levels of digital literacy when navigating the digital environment themselves;[[15]](#footnote-15) this can unintentionally result in the public dissemination of a child’s information. For example, a user’s individual privacy settings is commonly seen as a sufficient precautionary measure in itself to prevent information being shared too widely; unfortunately, many users do not realise how their information is disseminated is also subject to the privacy settings of other users. A user’s information can be shared beyond their privacy settings if shared by their ‘friends’ or ‘connections’ who have less rigorous privacy settings that allow the public to view ‘reposts’ and ‘likes’ of the original content.[[16]](#footnote-16)
4. Tech companies have been the subject of a number of serious data breaches in recent times. The nature of these breaches have raised doubts regarding the conduct of these companies[[17]](#footnote-17) and indicates that all information (including a child’s information) on a global online platform is vulnerable to theft and misuse.
5. The digital environment is still in its infancy and remains largely unregulated.[[18]](#footnote-18) It is, therefore, difficult to successfully anticipate the evolution of this environment and its effect on children’s rights unless nation states take measures to determine the parameters of its use domestically[[19]](#footnote-19) (and as a coalition globally[[20]](#footnote-20)).

***Impact on children’s rights***

1. These problematic behaviours arguably result in a number of current and prospective breaches of a child’s rights, both in the digital environment and beyond. There are three main categories of concern when considering the impact of the problematic behaviours outlined above:
   1. The protection of a child’s privacy, identity and data processing[[21]](#footnote-21)
   2. The intersection between the dissemination of a child’s information and the need to protect children from violence, sexual exploitation and other harm[[22]](#footnote-22)
   3. The impact of as yet unknown practices that may result in a breach of children’s rights.
2. The rights[[23]](#footnote-23) - and potential breaches - that can arise in relation to the first two categories has been considered in some detail therefore they will not be raised in this paper; however, the third category remains largely unexplored. One approach that may assist in anticipating potential breaches to children’s rights is an analysis of two key factors: (i) *who* might view, search or use a child’s personal information; and (ii) the *purpose(s)* for seeking out and utilising information sourced from the digital environment.
3. It has become increasingly common practice for prospective employers to conduct ‘social media screenings’ during the recruitment process. These processes can also be applied to children in a range of circumstances. Examples might include:
   1. Private education institutions may choose ‘screen’ parents’ profiles to determine the suitability of prospective students. This may impact on rights relating to non-discrimination,[[24]](#footnote-24) and access to education.[[25]](#footnote-25)
   2. Children aged 13-17 years are the first generation of children to have their personal information shared online from birth.[[26]](#footnote-26) Both public and private sector agencies are in a unique position to have access to lifelong digital records of a child’s personal information. This information has the potential be used to determine access to (including the restriction of) services such as social security,[[27]](#footnote-27) access to justice,[[28]](#footnote-28) and the provision of healthcare (including access to affordable insurance). It should be noted that any impact would extend beyond childhood which may lead to lifelong inequalities.
4. Additionally, it should be noted that are a number of barriers which impede the ability to identify and address these issues and the way in which they impact on children’s rights. These include:
   1. A lack of data regarding the dissemination of children’s information online[[29]](#footnote-29)
   2. Cultural responses to parenting[[30]](#footnote-30) and a lack of established methodologies to address these issues
   3. The application of welfare-driven approaches to child rights issues more broadly[[31]](#footnote-31)
   4. A lack of domestically entrenched legal protections for children[[32]](#footnote-32)
   5. Inadequate regulation of the digital environment.
5. Conclusion
6. All nation states that are a party to the International Bill of Rights generally, and the *Convention on the Rights of the Child* specifically, have an obligation to respect, protect and fulfil children’s rights. In this context, the challenges associated with balancing the rights of children and those of duty bearers (and other non-state actors) in the digital environment require an approach that is centred on meeting the principle of proportionality applied in international jurisprudence.[[33]](#footnote-33)
7. When considering the options available to nation states to influence the behaviour of their citizens to effect positive behavioural change, there are five policy levers[[34]](#footnote-34) that can be utilised by governments to implement initiatives and reforms to address issues associated with the dissemination of a child’s information by third parties:
8. Organisation: this lever refers to macro-level changes in location, magnitude, co-ordination and diversity of human and physical capital[[35]](#footnote-35)
9. Regulation: this lever operates by using ‘government power to enforce changes in behaviour’[[36]](#footnote-36) – both social and economic - through the enactment of legislation, regulations, guidelines and standards
10. Education: this lever focuses on the strategic dissemination of information to influence changes in the behaviour of individuals and organisations[[37]](#footnote-37)
11. Finance: the levers utilises mechanisms such as revenue generation and the allocation/distribution of funds[[38]](#footnote-38)
12. Incentives: Developing a system of incentives that are designed to encourage state and non-state actors to achieve desired outcomes.[[39]](#footnote-39)
13. There are a number of opportunities available to nation states to respect, protect and fulfil the rights of children by using the above levers, in collaboration with non-state actors, to guide reforms in this space. A preliminary list of possible opportunities is outlined in the table below:

|  |  |
| --- | --- |
| Opportunities | Policy Mechanism(s) |
| Increasing duty bearers’ awareness to the risks of third parties[[40]](#footnote-40) disseminating a child’s information online (e.g. an education program for expectant and new parents) [[41]](#footnote-41) | Education  Finance  Incentives |
| Increasing children’s awareness to the risks of third parties disseminating their information online[[42]](#footnote-42) | Education  Finance  Incentives |
| Invest in high quality research to produce data and identify best practice approaches as a foundation for policy development and reform | Education  Finance  Incentives |
| Introduction of legislation to regulate the digital environment in relation to the dissemination of a child’s information[[43]](#footnote-43) | Regulation |
| Collaboration and co-design with tech companies to develop a child-safe digital environment[[44]](#footnote-44) | Regulation  Education  Incentives |

1. The proposed General Comment offers an opportunity to provide guidance to nation states regarding how they can promote effective, co-ordinated, evidence-based approaches to address the dissemination of a child’s information by a third party online. The measures, as outlined above, not only provide policy and law makers with various methods to address this issue, but also have the potential to be developed in concert with broader, complementary measures that impact the digital environment more broadly. This will ensure that actions taken in relation to the digital environment are coordinated, comprehensive and cost effective.
2. Nation states should be encouraged to develop measures that clarify duty bearers’ responsibility to children in the digital environment. Measures should also be applied to tech companies, in recognition of their status as powerful non-state actors who enjoy operating in a largely unregulated digital environment. Furthermore, any such measures should focus on giving full effect to children’s rights as outlined in the *Convention on the Rights of the Child* and develop policy initiatives using an ‘interests’ model of child rights, as opposed to the welfare model which is too often adopted.
3. The decision to enter the digital environment, while opening the door to many opportunities, also invites a number of significant risks, both online and offline. Nation states, in their role as a duty bearer, have an obligation to respect a child’s right to choose when they enter the digital environment and protect those children from the adverse effects of that environment as a result of third party actions.

1. Cassandra Seery is an Associate Lecturer in Law at Deakin University, Australia. Her work focuses on child rights and policy and has presented internationally on the role of international child rights in a domestic context. She was formally a public servant in Victoria specialising in vulnerable children and Aboriginal affairs and is a current member of the Australian Child Rights Taskforce and the Bravehearts Inc. Research Advisory Council. [↑](#footnote-ref-1)
2. See, for example Australian Child Rights Taskforce, *The Children’s Report Australia’s NGO coalition report to the United Nations Committee on the Rights of the Child, November* 2018, 21. [↑](#footnote-ref-2)
3. This would include parents, care givers, family members, those employed to meet the needs of children and corporations that provide platforms in the digital environment. [↑](#footnote-ref-3)
4. London School of Economics, ‘What do parents think, and do, about their children’s online privacy?’, *Parenting for a Digital Future: Survey Report 3* (2018), 5<<http://www.lse.ac.uk/media-and-communications/assets/documents/research/preparing-for-a-digital-future/P4DF-Report-3.pdf> >. [↑](#footnote-ref-4)
5. This would exclude criminal conduct. [↑](#footnote-ref-5)
6. Alternatively, this will include guardians who have parental responsibility for a child. [↑](#footnote-ref-6)
7. See Zachary Loeb, ‘Technology giants didn’t deserve public trust in the first place’, *The Conversation* (19 November 2018) <<https://theconversation.com/technology-giants-didnt-deserve-public-trust-in-the-first-place-106989>> : ‘Using any technology – from a knife to a computer – carries risks, but as technological systems increase in size and complexity the scale of these risks tends to increase as well.’ [↑](#footnote-ref-7)
8. This can include anything that is considered a copyright-able work such as a person’s comments, photos, videos, individual posts, etc. [↑](#footnote-ref-8)
9. Facebook, *Terms of Service:* *The permissions you give us* (accessed 13 May 2019) <[https://www.facebook.com/terms.php 3](https://www.facebook.com/terms.php%203)>. [↑](#footnote-ref-9)
10. Ibid. [↑](#footnote-ref-10)
11. Consider, for example, delays in posting items for sale on Facebook Marketplace, where individuals use key words that may indicate a prohibited transaction item (such as an animal) is attempting to be sold. [↑](#footnote-ref-11)
12. See, for example, Andrew Quodling, ‘Shadow profiles - Facebook knows about you, even if you’re not on Facebook’, *The Conversation* (13 April 2018) <<https://theconversation.com/shadow-profiles-facebook-knows-about-you-even-if-youre-not-on-facebook-94804>. [↑](#footnote-ref-12)
13. This includes the Cambridge Analytica scandal, which saw the illegal collection of over 50 million Facebook users’ information; devices that record and monitor users conversations and interactions; etc. See also Zachary Loeb, ‘Technology giants didn’t deserve public trust in the first place’, *The Conversation* (19 November 2018) <<https://theconversation.com/technology-giants-didnt-deserve-public-trust-in-the-first-place-106989> >. [↑](#footnote-ref-13)
14. See, for example, David Glance, ‘It’s impossible for Facebook users to protect themselves from data exploitation’, *The Conversation* (23 March 2018) <<https://theconversation.com/its-impossible-for-facebook-users-to-protect-themselves-from-data-exploitation-93800>>. Additionally, while it is beyond the scope of this submission, further consideration should be given to when children can legally create profiles on social media platforms. It is questionable that social media platforms can allow children under the age of 18 to create profiles, with the minimum age currently being set at 13 years of age (which is generally self-certified). Worse still, it appears that this ‘age limit’ is not actively enforced by platforms such as Facebook and Instagram, although steps are being taken to do so. It has also been noted that Facebook has been purposefully attempting to attract children [under the age of 13](https://techcrunch.com/2018/07/19/facebok-under-13/) through its [Messenger Kids App](https://www.nytimes.com/2017/12/04/technology/facebook-messenger-kids.html), which was introduced in 2017. It has also been widely reported that Facebook CEO Mark Zuckerberg does not believe an age limit should exist (<http://fortune.com/2011/05/20/zuckerberg-kids-under-13-should-be-allowed-on-facebook/>). This raises significant issues regarding informed consent, the forms of advertising children are exposed to (such as gambling, alcohol, etc), public safety concerns regarding screen-time for children, and the lack of protections regarding fake news and other dangerous content. This is arguably the active exploitation of a vulnerable group – in respect of their legal rights and remedies – who are ill-equipped to identify, report and litigate any breaches that may arise. [↑](#footnote-ref-14)
15. London School of Economics, ‘What do parents think, and do, about their children’s online privacy?’, *Parenting for a Digital Future: Survey Report 3* (2018) <<http://www.lse.ac.uk/media-and-communications/assets/documents/research/preparing-for-a-digital-future/P4DF-Report-3.pdf> >. [↑](#footnote-ref-15)
16. Consider, the example of an Australian man who posted a picture of his naked toddler in the bath on Facebook, thinking it would only be seen by friends and family, only to discover 3000 strangers had clicked on and ''liked'' the image: <https://www.smh.com.au/technology/parents-warned-of-dangers-in-posting-childrens-images-online-20140330-35rtv.html>. [↑](#footnote-ref-16)
17. Consider, for example, security issues allowing hackers to access user information without permission (including weak authentication measures), so called ‘self-deleting’ message applications that have been prone to issues such as: the ability to save images or videos, gathering geolocation information, issues associated with ‘find friends’ functions and hacking attempts, etc. [↑](#footnote-ref-17)
18. This is slowly changing; the EU General Data Protection Regulation (EU) 2016/679 is a good example of major changes in this space. [↑](#footnote-ref-18)
19. Consider, for example the Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505, which is the legal framework tech companies (who are overwhelming based in the United States of America) use as the foundation of their interactions with children. [↑](#footnote-ref-19)
20. This is something that is slowly being acknowledged by nation states – New Zealand Prime Minister Jacinda Ardern is seeking to address the streaming of extreme violent content online via a global approach known as the ‘Christchurch Call’. [↑](#footnote-ref-20)
21. Right to privacy: *Convention on the Rights of the Child*, article 16. See also *International Covenant on Civil and Political Rights* article 17, *Universal Declaration of Human Rights* articles 12 and 22(1). [↑](#footnote-ref-21)
22. *Convention on the Rights of the Child* articles 19(1) and 34. This could also cover cruel, inhuman or degrading treatment under article 7 of the *International Covenant on Civil and Political Rights*, article 5 *Universal Declaration of Human Rights*, and article 37(2) of the *Convention on the Rights of the Child*. Consider also the right to life under Article 6 of the *Convention on the Rights of the Child* and the corresponding obligations. [↑](#footnote-ref-22)
23. While acknowledging that a wide range of rights could be affected, this discussion is confined to those in the International Bill of Rights and the *Convention on the Rights of the Child*. [↑](#footnote-ref-23)
24. Article 2 of the *Convention on the Rights of the Child*, article 2 of the *International Covenant on Civil and Political Rights*, article 2 of the *Universal Declaration of Human Rights*, and article 2 of the *International Covenant on Economic, Social and Cultural Rights.*  [↑](#footnote-ref-24)
25. Articles 23, 28, 29 of the *Convention on the Rights of the Child*; article 13 of the *International Covenant on Economic, Social and Cultural Rights.* [↑](#footnote-ref-25)
26. This is via the dissemination of personal information by third parties but can also include those who now engage with the digital environment directly (e.g. through the creation of an online account). [↑](#footnote-ref-26)
27. Article 3 of the *International Covenant on Civil and Political Rights*, article 3 of the *International Covenant on Economic, Social and Cultural Rights*, and article 22 of the *Universal Declaration of Human Rights.* [↑](#footnote-ref-27)
28. Article 26 of the *International Covenant on Civil and Political Rights*; article 7 *Universal Declaration of Human Rights.* [↑](#footnote-ref-28)
29. Recently, efforts have been made in this space, but it still remains largely unexplored. See London School of Economics, ‘What do parents think, and do, about their children’s online privacy?’, *Parenting for a Digital Future: Survey Report 3* (2018) <<http://www.lse.ac.uk/media-and-communications/assets/documents/research/preparing-for-a-digital-future/P4DF-Report-3.pdf> >. [↑](#footnote-ref-29)
30. See, for example, Australian Institute of Family Studies, ‘Differential parenting of children from diverse cultural backgrounds attending child care’ (2007) *Research Paper 39* <<https://aifs.gov.au/publications/differential-parenting-children-diverse-cultural-bac/introduction>>; Marc H. Bornstein, ‘Cultural Approaches to Parenting’ (2012) 12(2-3) *Parent Sci Pract.* 212–221 <<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3433059/>>; Joseph Roundtree Foundation, *Parenting and the different ways it can affect children’s lives: research evidence* (2007) <<https://www.jrf.org.uk/sites/default/files/jrf/migrated/files/2132-parenting-literature-reviews.pdf>>. [↑](#footnote-ref-30)
31. This may also include a reluctance to address potential conflicts that may arise between a child’s right and a parent’s right (as either an individual or a duty bearer). [↑](#footnote-ref-31)
32. This includes both positive and negative rights. [↑](#footnote-ref-32)
33. Consider, for example, the application of the legitimate aim and purpose test in *S.A.S v France* (application No. 43835/11) (1 July 2014) and discussion in Juan Cianciardo, ‘The Principle of Proportionality: The Challenges of Human Rights’ (2010) 3(1) *Journal of Civil Law Studies* 177, 179. [↑](#footnote-ref-33)
34. F Grace et al, ‘An analysis of policy levers used to implement mental health reform in Australia 1992-2012’ (2015) *BMC Health Services Research*. See also Australian Public Service Commission, *Changing behaviour: A public policy perspective*, archived publications < <https://www.apsc.gov.au/changing-behaviour-public-policy-perspective> >. [↑](#footnote-ref-34)
35. F Grace et al, ‘An analysis of policy levers used to implement mental health reform in Australia 1992-2012’ (2015) *BMC Health Services Research*. [↑](#footnote-ref-35)
36. Ibid. [↑](#footnote-ref-36)
37. Ibid. [↑](#footnote-ref-37)
38. Ibid. [↑](#footnote-ref-38)
39. Ibid. Please note that the definition ‘incentive’ is used in lieu of the term ‘payment’. [↑](#footnote-ref-39)
40. Adopting the rationale and wording of article 24(2)(e) of the *Convention on the Rights of the Child*: ‘ensure that…parents and children, are informed, have access to education and are supported in the use of basic knowledge of…’ [↑](#footnote-ref-40)
41. Consider article 14(2) of the *Convention on the Rights of the Child* and the focus on the duties of the parent to ‘provide direction to the child in the exercise of his or her right in a manner consistent with the evolving capacities of the child’. [↑](#footnote-ref-41)
42. It is important to note that this measure will have an intergenerational impact given that these children will grow to become the next generation of duty bearers. [↑](#footnote-ref-42)
43. Regulating the digital environment will no doubt raise issues concerning a parent’s right to post their child’s information online and the question of whether – or to what extent – this should be restricted. Given restricting a parent’s right to post online does not infringe on their right to parent a child, such a restriction could be considered a reasonable and legitimate restriction in order to fulfil their obligations as duty bearer. [↑](#footnote-ref-43)
44. Measures could include: disabling facilities that allow ‘shadow profiles’ to be developed for children, introduction of prompts prior to posting photos or videos of children, disable sharing of content that includes a child’s information to the owner-user, disable photo ‘tagging’ of children, allow children to ‘disallow’ posts made by third parties that include their personal information, introduce mandatory reporting for tech companies etc. [↑](#footnote-ref-44)