



Submission to the South African Law Commission

## Discussion Paper 149 on Sexual Offences: Pornography and Children

Attention:

Ms. D. Clark; [dclark@justice.gov.za](mailto:dclark@justice.gov.za)

30 July 2019

For further information please contact:

Ms. Anri van der Spuy, Senior Researcher,  
Research ICT Africa

[avanderspuy@researchictafrica.net](mailto:avanderspuy@researchictafrica.net); +27 21 447 6332

## Executive Summary

Research ICT Africa (RIA) and the Association for Progressive Communications (APC) welcome this opportunity to jointly submit written comments on the South African Law Commission (SALRC) *Discussion Paper 149 on Sexual Offences: Pornography and Children*, published in April 2019.

The *Discussion Paper* solicits views and comments on proposed amendments to the legislative framework that currently applies to children in respect of ‘pornography’, and forms part of an overarching investigation into the review of all sexual offences found in common law and statute. Among other things, *Discussion Paper 149* is concerned with improving ‘the regulation of pornography, including on the Internet’. It covers five areas of concern:

- access to or exposure of a child to pornography;
- creation and distribution of child sexual abuse material;
- explicit self-images created and distributed by a child;
- grooming of a child and other sexual contact crimes associated with pornography or which are facilitated by pornography or child sexual abuse material; and
- investigation, procedural matters and sentencing.

RIA and APC make this joint submission in the public interest to ensure that the Internet, and access to it, can be a force for good in South Africa rather than becoming a tool which benefits some and leaves marginalised or vulnerable communities (including children) further behind. We thank the SALRC for its work in compiling the *Discussion Paper*, and also for providing an opportunity for further input from stakeholders.

Like the Commission (c.f. para 1.28 of Chapter 1 of *Discussion Paper 149*), we firmly believe that public consultation and participation are vital, as no stakeholder group, legislator or regulator can effectively regulate online content or activities alone. Enabling the participation and input from civil society, academia, the private sector, technical community and users (including children) is likely to lead to a much stronger, more effective responses to these evolving problems that accompany our exposure and inclusion in a global information society.

As access to the Internet increases in South Africa, users, including children, are exposed to new or different threats and risks in addition to the ones they face ‘offline’. While these risks can be significant, they need to be considered in the context of existing offline risks and broader social changes that span both online and offline contexts. Access to the Internet does entail that users (including children) might be exposed to content that might be disturbing. It can also expose children to online harassment or bullying. However, access to the Internet can also help children understand and respond to the risks that they face offline and online, inform them about how to avoid risk, find help when they are exposed to negative online experiences, report abuses, and connect with other children who may have had similar experiences.

We are concerned that the *Discussion Paper* tends to conflate risk with harm and, in doing so, may constrain the development and participation of children through technology in a globalised information society. We are particularly concerned about the proposal to require a default setting on devices to prevent children from having access to content which is (subjectively) deemed to be potentially harmful. This provision is not only technologically determinist and impractical from an implementation point of view, but wholly neglects children's rights to information, health, expression, and freedom of association. In trying to protect children, it risks restricting children's rights in a manner that would arguably fail to meet constitutional thresholds of legitimacy and proportionality.

While the *Paper* acknowledges the fact that some children will react differently to online risk, it still recommends overarching policy responses that will be overly restrictive to most young users whilst inadequate or inappropriate for others. We believe that harm and risk need to be thoroughly understood in order to design and target encompassing interventions at children who might be more susceptible or vulnerable of risk. One of the most significant policy challenges in curtailing potential risks that accompany children's (and adults') digital inclusion is the lack of data pertaining to how children access and use the Internet, including their preferences, needs, concerns, perceptions and experiences. Without gathering such data, our policymakers are unable to make assumptions about children's online risks. Relying on assumptions of the risks children face online without gathering such data means that our policymakers are unable to make informed decisions.

We would like also to confirm our availability for making oral representations should the SALRC decide to hold public hearings.

### **About Research ICT Africa**

Research ICT Africa (RIA) is a regional digital policy and regulation think tank based in Cape Town and active across Africa and the global South. It conducts research on digital economy and society that facilitates evidence-based and informed policymaking for improved access, use and application of information and communication technologies (ICTs) for social development and economic growth. RIA also has a dedicated digital policy unit which specialises in Internet governance, digital rights, cybersecurity, gender, innovation (including artificial intelligence and the Internet of Things), and data justice. Understanding the needs and digital challenges of marginalised communities – including women, youth, children, the elderly, and people in rural areas, for example – form an integral part of RIA's work.

### **About the Association for Progressive Communications**

The Association for Progressive Communications (APC) is a membership-based network of organisations founded in 1990, who work collaboratively to empower and support organisations, social movements and individuals through the use of ICTs for human rights and development. APC's vision is for all people to have easy and affordable access to a free and open Internet to improve their lives

and create a more just world. APC works virtually with almost 40 staff from over 20 countries and an administrative office in South Africa.

### **Acknowledgements**

This submission was drafted and prepared by Anri van der Spuy, Alex Comninos, Anriette Esterhuysen, and Deborah Brown, with valuable inputs, contributions and revisions from other RIA and APC staff members. Any errors or omissions of course remain the authors' own.

This submission was made possible by the support received from Canada's International Development Research Centre (IDRC).

## Introduction

The Internet is a global 'network of networks' which enables communication between networks using certain protocols to communicate across layers on a global and mostly public scale. Taken as a whole, the Internet has no central authority and essentially remains non-hierarchical and decentralised;<sup>1</sup> making it a particularly difficult governance challenge. It is more than the sum of its technological parts; a network of interactions and relationships which extends beyond technology and across borders, across cultures, as well as across ages.<sup>2</sup>

In 2015, the United Nations' *2030 Agenda for Sustainable Development* acknowledged the importance of ICTs like the Internet for promoting sustainable development.<sup>3</sup> Since then, universal access to the Internet is often cited as a precondition for sustainable development. And the position of children in the burgeoning information society was recognised in 2003 during the first phase of the World Summit on the Information Society (WSIS):<sup>4</sup>

*We recognize that young people are the future workforce and leading creators and earliest adopters of ICTs. They must therefore be empowered as learners, developers, contributors, entrepreneurs and decision-makers. We must focus especially on young people who have not yet been able to benefit fully from the opportunities provided by ICTs. We are also committed to ensuring that the development of ICT applications and operation of services respects the rights of children as well as their protection and well-being.*

Despite this focus on the empowering potential of ICTs, children's roles, rights and needs are often neglected in the global digital policy arena, although human rights mechanisms and intergovernmental organisations have recently started to pay more attention these issues.<sup>5</sup> When children are acknowledged in digital policy arenas, it tends to be in the context of 'child online protection' rather than an empowering approach of respecting and promoting children's rights.<sup>6</sup> Policymakers also tend to look at certain harmful content in isolation, rather than consider broader and interrelated challenges

---

<sup>1</sup> Kleinwächter, W. (2014) "NETmundial: Watershed in Internet Policy Making?" In: Drake, W.J. & Price, M. (Eds.) (2014) *Beyond NETmundial: The Roadmap for Institutional Improvements to the Global Internet Governance Ecosystem*. Available at: [http://www.global.asc.upenn.edu/app/uploads/2014/08/BeyondNETmundial\\_FINAL.pdf](http://www.global.asc.upenn.edu/app/uploads/2014/08/BeyondNETmundial_FINAL.pdf).

<sup>2</sup> Van der Spuy, A. (2017) *What if we all governed the Internet? Advancing Multistakeholder Participation in Internet Governance*. Paris: UNESCO. Available at: [https://en.unesco.org/sites/default/files/what\\_if\\_we\\_all\\_governed\\_internet\\_en.pdf](https://en.unesco.org/sites/default/files/what_if_we_all_governed_internet_en.pdf).

<sup>3</sup> UNGA (2015) A target for universal and affordable access to ICTs in least developed countries (LDCs) by 2020 is contained in goal 9c of the *Agenda*, while ICTs is included in goal 17 as an enabling means of implementation. UNGA. (2015, October 21). *Transforming our world: The 2030 Agenda for Sustainable Development (Resolution A/Res/70/1)*. Available at: [http://www.un.org/ga/search/view\\_doc.asp?symbol=A/RES/70/1&Lang=E](http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E).

<sup>4</sup> WSIS (2003) *Geneva Declaration of Principles and Plan of Action*. Geneva: ITU. Available at: <https://www.itu.int/net/wsis/docs/promotional/brochure-dop-poa.pdf>.

<sup>5</sup> e.g., UN Human Rights Council (2016). *Rights of the child: information and communications technologies and child sexual exploitation (A/HRC/31/L.9/Rev.1)*. Available at: <http://daccess-ods.un.org/access.nsf/Get?Open&DS=A/HRC/31/L.9/Rev.1&Lang=E>. UNICEF. The ITU also developed, through a multistakeholder initiative, the *Guidelines for Industry on Child Online Protection*. Available at: [https://www.unicef.org/csr/ict\\_resources.html](https://www.unicef.org/csr/ict_resources.html).

<sup>6</sup> Livingstone, S., Carr, J. & Byrne, K. (2015, November). *One in three: Internet governance and children's rights*. Global Commission on Internet Governance, 22. Available at: [http://eprints.lse.ac.uk/68516/1/Livingstone\\_European%20Research%20on%20Children\\_2018.pdf](http://eprints.lse.ac.uk/68516/1/Livingstone_European%20Research%20on%20Children_2018.pdf).

related to the governance of online content and the responsibilities of platforms and other content intermediaries.

While some governments have started investigating ways of governing online harms,<sup>7</sup> no country has yet been able to address online harms in a single or coherent way. Perhaps more worrying, even with policies or legislation in place, implementation is often lacking, impractical, or sometimes has unintended consequences which might cause more harm than good where children's rights and opportunities are concerned.

Digital policy challenges apply globally, but are especially difficult to address in developing country contexts like South Africa. With only 53% of the South African population online,<sup>8</sup> significant access discrepancies persist between rural or urban areas, between women and men, between poor or wealthier segments, between literate or illiterate people, and between children, adults and the elderly. For those South Africans who are online, Internet use is often intermittent and passive. A relatively small number of South Africans actually have the skills or resources to participate meaningfully online.<sup>9</sup>

Both supply- and demand-side barriers have an impact on South Africans' digital inclusion, and require encompassing societal changes, government intervention, and/or development initiatives to overcome.<sup>10</sup> Because Internet availability has outpaced adoption in parts of the country, demand-side barriers are especially important. A lack of relevant skills and content is a particular problem, with nine of South Africa's eleven official languages being underrepresented online. English and Afrikaans remain the only languages with a strong online presence on news websites and platforms.<sup>11</sup>

Because barriers to access and meaningful use are so difficult to address, policymakers tend to neglect them and focus on symptomatic challenges rather than underlying ones. Challenges also continue to evolve at a significant pace, continuously introducing new governance and regulatory challenges, with the growing importance of technologies that underpin the so-called Fourth Industrial Revolution (4IR), like the Internet of Things (IoT), Artificial Intelligence (AI), and additive manufacturing.

On this note, President Cyril Ramaphosa<sup>12</sup> and other policymakers' interest in and support for the 4IR – a notion developed and driven by the World Economic Forum (WEF)<sup>13</sup> – is an interesting example of how policymakers tend to embrace the untested potential of new technologies without addressing

---

<sup>7</sup> HM Government (2019, April) *Online Harms White Paper* (CP 57). Gov.uk/Crown. Available at: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/793360/Online\\_Harms\\_White\\_Paper.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf).

<sup>8</sup> Gillwald, A. Mthobi, O. & Rademan, B. (2019) *The State of ICT in South Africa*. Research ICT Africa. Available at: [https://researchictafrica.net/wp/wp-content/uploads/2018/10/after-access-south-africa-state-of-ict-2017-south-africa-report\\_04.pdf](https://researchictafrica.net/wp/wp-content/uploads/2018/10/after-access-south-africa-state-of-ict-2017-south-africa-report_04.pdf).

<sup>9</sup> *ibid.*

<sup>10</sup> Van der Spuy, A. & Souter, D. (2018) *Women's Digital Inclusion: Background Paper for the G20*. Geneva: APC & the Internet Society. Available at: [https://www.apc.org/sites/default/files/WomensDigitalInclusion\\_BackgroundPaper.pdf](https://www.apc.org/sites/default/files/WomensDigitalInclusion_BackgroundPaper.pdf).

<sup>11</sup> Freedom House (2018) *Freedom on the Net 2018: South Africa*. Available at: <https://freedomhouse.org/report/freedom-net/2018/south-africa>.

<sup>12</sup> e.g. his SONA on 20 June 2019, in which he made two references to the 4IR.

<sup>13</sup> Schwab, K. (2016, January 16) *The Fourth Industrial Revolution: What it is, how to respond*. World Economic Forum. Available at: <https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/>.

underlying or foundational challenges. South Africa's adoption of the 4IR mantra has been criticised due to limited corresponding evidence as to what the 4IR actually means, less engagement with how it supposedly impacts countries in different stages of development, and no understanding of how especially developing countries and potentially vulnerable communities like children can benefit from and not be harmed by it. Given that South Africa that large numbers of South Africans do not even enjoy the benefits of the second and third industrial revolution, South Africa's children are likely unprepared for and unlikely to benefit from the technologies that constitute the 4IR.<sup>14</sup>

Besides this focus on future technologies and the 4IR, South African policymakers have not shown consistent interest in addressing current digital challenges like those faced by children. As the Internet and digital inclusion increasingly becomes a precondition for participation in today's society – from the provision of e-government services like access to an identity document to procuring social benefits, performing work, accessing finance, or gaining education – it is critical that South Africans of all ages are able to safely participate online. The Internet should be a space which enables users – whether children or adults – to exercise their rights without being exposed to undue harms or risks.

We are concerned that the SALRC's *Paper* seems to focus on safety and protection whilst neglecting children's rights to freedom of expression, access to information, health, and freedom of association. These are not mutually exclusive. The SALRC arguably adopts an overly protectionist approach to providing a safe environment online while neglecting the need to promote children's rights and the empowering potential of technology.

With this background in mind, and before submitting comments on specific sections and clauses of *Discussion Paper 149*, we highlight the following overarching concerns. These comments relate to the SALRC's *Discussion Paper* and efforts to regulate specifically online sexual offences and/or sexual offences facilitated through or by the use of technology where children are concerned:

- Governing online content is difficult from a practical perspective due to the nature of the Internet as a network of networks.<sup>15</sup> For governance responses to be effective, broad participation and collaboration with the private sector, technical community, civil society, and users is needed. Such **multistakeholder** approaches are useful in enabling a higher degree of openness, transparency, and the broad-based collaboration and equal participation of all those affected.<sup>16</sup> This includes children themselves.

---

<sup>14</sup> Gillwald, A. (2019, July 4) *4IR in SA is too important to remain the domain of the elite*. Business Day (opinion piece). Available at: <https://www.businesslive.co.za/bd/opinion/2019-07-04-4ir-in-sa-is-too-important-to-remain-the-domain-of-the-elite/>; Unwin, T. (2019, March 9) *Why the notion of a Fourth Industrial Revolution is so problematic*. Tim Unwin's blog. Available at: <https://unwin.wordpress.com/2019/03/09/why-the-notion-of-a-fourth-industrial-revolution-is-so-problematic/>.

<sup>15</sup> Kleinwächter, 2014, *ibid*.

<sup>16</sup> World Bank (2016) *World Development Report 2016: Digital Dividends*. Available at: [http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2016/01/13/090224b08405ea05/2\\_0/Rendered/PDF/World0developm0000digital0dividends.pdf](http://www-wds.worldbank.org/external/default/WDSContentServer/WDSP/IB/2016/01/13/090224b08405ea05/2_0/Rendered/PDF/World0developm0000digital0dividends.pdf); Gill, L.; Redeker, D. & Gasser, U. (2015) *Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights*. Research Publication No. 2015-15. Available at: <https://cyber.harvard.edu/node/99209>.

- We commend the SALRC for recognising the risks that accompany digital inclusion, but are concerned about the apparent failure to consider the importance of adopting a more **empowering** approach to children’s rights in the digital age. South Africa cannot afford to focus solely on risk, or the country’s children will be excluded from the opportunities that also accompany Internet use and future technologies (like the 4IR) – something we can ill afford.
- We encourage the SALRC to closely interrogate the binary distinction it makes between ‘offline’ and ‘online’ harms. **Online and offline** experiences are closely related and interlinked,<sup>17</sup> with the effects of varied human rights infringements online not only echoing, extending into and mingling with offline contexts,<sup>18</sup> but unsurprisingly having roots in offline realities and norms.<sup>19</sup> The legacy of ‘offline’ inequality means legislative change alone is insufficient. We therefore argue that an empowering approach to children’s rights is crucial. This includes a focus on **education and digital literacy** (e.g., how to use social media safely).
- We are particularly concerned about and strongly disagree with the intention to require a **default setting** on devices to prevent children from having access to potentially harmful content. This provision is not only technologically determinist and impractical from an implementation point of view, but wholly neglects children’s rights to freedom of association, freedom of expression, and access to information. In trying to protect children, it risks limiting children’s rights in a manner that would arguably fail to meet the Constitutional threshold of being legitimate, necessary and proportional to the aim of the limitation.
- We encourage the SALRC to draw a clearer distinction between **risk and harm**, as the potential prevalence or existence of online risks does not necessarily lead to experiences of harm.<sup>20</sup> Mere exposure to certain content also does not necessarily result in harm. Nevertheless, the SALRC seems to conflate risk with actual harm in the paper.<sup>21</sup> Without properly differentiating between risk and harm, efforts like those of the SALRC to address supposed harms can actually restrict children’s rights.<sup>22</sup>

---

<sup>17</sup> c.f. Van der Spuy, A. & Aavriti, N. (2018) *Mapping Research in Gender and Digital Technology*. Ottawa: IDRC & APC. Available at: [https://www.apc.org/sites/default/files/IDRC\\_Mapping\\_0323\\_0.pdf](https://www.apc.org/sites/default/files/IDRC_Mapping_0323_0.pdf).

<sup>18</sup> Dad, N. & Khan, S. (2017, January 12) Naila Rind killed herself because Pakistan’s cybercrime laws failed her, Digital Rights Foundation (open letter to Minister). *Dawn*. [www.dawn.com/news/1306976/naila-rind-killed-herself-because-pakistans-cybercrime-laws-failed-her](http://www.dawn.com/news/1306976/naila-rind-killed-herself-because-pakistans-cybercrime-laws-failed-her); Digital Rights Foundation (2016) *Surveillance of Female Journalists of Pakistan*. Available at: [www.digitalrightsfoundation.pk/wp-content/uploads/2017/02/Surveillance-of-Female-Journalists-in-Pakistan-1.pdf](http://www.digitalrightsfoundation.pk/wp-content/uploads/2017/02/Surveillance-of-Female-Journalists-in-Pakistan-1.pdf); Pasricha, J. (2016b) “Violence” Online in India: Cybercrimes Against Women & Minorities on Social Media. N/A: Feminism in India. Available at: [www.feminisminindia.com/wp-content/uploads/2016/05/FII\\_cyberbullying\\_report\\_website.pdf](http://www.feminisminindia.com/wp-content/uploads/2016/05/FII_cyberbullying_report_website.pdf).

<sup>19</sup> Shephard, N. (2016). *Big data and sexual surveillance (APC issue paper)*. Johannesburg: APC. Available at: [www.apc.org/en/system/files/BigDataSexualSurveillance\\_0.pdf](http://www.apc.org/en/system/files/BigDataSexualSurveillance_0.pdf).

<sup>20</sup> Livingstone, S. & Helsper, E. (2013) Children, internet and risk in comparative perspective. *Journal of Children and Media*, vol. 7 (1): 1-8; Haddon, L. & Livingstone, S. (2014) “The Relationship between Offline and Online Risks” In: von Feilitzen, C. & Stenersen, J., (eds.) *Young people, media and health: risks and rights*. The Clearinghouse Yearbook (2014). Goteborg: Nordicom.

<sup>21</sup> Livingstone, S. (2014) “Risk and harm on the internet” In: Jordan, A. & Romer, D., (eds.) *Media and the well-being of children and adolescents*. Oxford: Oxford University Press.

<sup>22</sup> Livingstone, S. (2009) Maximising opportunities and minimising risks for children online: from evidence to policy. *Intermedia*, vol. 37 (4): 50-53.

- One of the most significant policy challenges in curtailing potential risks that accompany children's (and adults') digital inclusion is the **lack of data** pertaining to how children access and use the Internet, including their preferences, needs, concerns, perceptions and experiences. Without gathering such data, our policymakers are unable to make assumptions about children's online risks. And they are even less able to develop policies on the basis of assumptions of the supposed risks children face online. Local policymakers are unlikely to be able to make any reasonable inference from even conservative statistics from other contexts (especially from the global North, from where the limited data available comes).
- Harm and risk need to be thoroughly understood in order to design and **target policy interventions** at specific children who might be more susceptible or vulnerable of risk. Little work has also been done to investigate how children can use the Internet to understand, seek help, advice and find solutions for harms they face in the offline world. Filtering children's Internet access with the aim of protecting them from perceived risks could undermine their ability to use the Internet to empower themselves; to seek information and advice in addressing the harms they could face. An Internet filter on a device, for example, could block Internet content about gender-based violence, sexual abuse, sexual health and education by mistakenly identifying it as sexual content. This lack of evidence leads to a tendency to recommend generic or blanket policies that may be insufficient for some children whilst being too restrictive for others.<sup>23</sup> We strongly encourage the SALRC to support the gathering of more research to provide a proper understanding not only the factors that may make some South African children in particular more vulnerable to harm from online risks, but also the supporting environments they have or do not have to help them deal with such potential exposure to online risk.
- While we note the recommendation that 'content providers' should 'take greater responsibility', we urge the SALRC to consider differentiating between **the size of a provider or platform, the nature of the platform** (e.g., platforms that merely host content, platforms that actively create content, or platforms that moderate or curate content) **and their related obligations**. While all businesses have the responsibility to protect and respect human rights regardless of their size, sector, operational context, ownership and structure, larger content providers or platforms arguably have different levels of responsibility. The scale and complexity of the means through which platforms or providers meet responsibilities, for instance, may vary according to these factors and with the severity of the platform or provider's potential impact on human rights.<sup>24</sup>
- We endorse the notion that warning messages (along with terms and conditions for consent) should, as far as is reasonably possible for platforms, be available in countries' official **languages**. As noted, nine of South Africa's eleven official languages are underrepresented online.<sup>25</sup> The lack

---

<sup>23</sup> *ibid.*

<sup>24</sup> OHCHR (2011). Guiding Principles on Business and Human Rights. Available at: [https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR\\_EN.pdf](https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf).

<sup>25</sup> Freedom House, 2018, *ibid.*

of relevant content in users' home language is a significant barrier to meaningful Internet access and use.<sup>26</sup>

- While we commend the SALRC for taking the rights of potential victims (or data subjects) seriously as far as **evidentiary issues** or the storage of potentially unlawful content is concerned, we argue for an exception in that anonymised content should be made available for researchers to better understand the incidence, design, prevalence and responses to online harms like those addressed by *Discussion Paper 149*. And because social media platforms are sometimes used to record and raise awareness of human rights violations (e.g., war crimes), content cannot simply be deleted. It must be safely archived and kept for evidentiary and research purposes.<sup>27</sup>

Besides these general comments, we now respectfully submit comments in response to specific sections and clauses of *Discussion Paper 149*. **Note that given RIA and APC's focus on telecommunications and digital policy, we focus our submissions on sections that specifically relate to technology (particularly the Internet) and/or children's use thereof.** While our comments may appear repetitive, we thought it may be helpful to use the same structure used by the SALRC in its *Discussion Paper* rather than clustering our comments.

## COMMENTS ON SPECIFIC PROVISIONS OF THE SALRC'S *DISCUSSION PAPER 149*

### Glossary – definition of 'Internet':

While we agree with the definition proposed for 'Internet' considering the growing use of the Internet Protocol, we think the terms TCP/IP (as the Internet's own language) should also be defined in the glossary. One suggestion is 'Transmission Control Protocol/Internet Protocol as a suite of communication protocols used to interconnect network devices on the Internet, or as a communications protocol in a private network such as an intranet or an extranet'. We note that 'Internet' and 'internet' are used interchangeably throughout *Discussion Paper 149*, and would like to point out that these terms have somewhat different meanings.

We also submit that other broader and closely related terms should also be included in the glossary in order to encompass the societal impacts of the Internet, including terms like 'information and communications technology' (ICT) and the 'Information Society'.

---

<sup>26</sup> Gillwald, Mothobi & Rademan, 2019, *ibid*.

<sup>27</sup> Van der Spuy, A. (2019b) *The Christchurch Call could potentially be used to clamp down on legitimate political dissent in Africa*. Daily Maverick (opinion piece). Available at: <https://www.dailymaverick.co.za/article/2019-05-20-the-christchurch-call-could-potentially-be-used-to-clamp-down-on-legitimate-political-dissent-in-africa/>.

Other words we believe should be defined (also in reference to existing legislation) – as we indicate later in this document – include ‘service provider’, ‘content provider’, and ‘electronic communication service providers’.

### Executive Summary – para 2:

We commend the SALRC for recognising the risks that accompany ‘mass media’ in general and digital inclusion in particular, but we are concerned about the apparent failure to consider the importance of adopting a more empowering approach to children’s rights in a digital age.

While we take note that the SALRC explains its focus on the ‘negative outcomes or risks associated with the use of ICT’s (*sic*) on the lives of children’ (Chapter 1, section 1.2), we caution that the positive and empowering potential of digital inclusion and Internet use should not be neglected. A primary focus on risks could cause more harm than benefit by limiting children’s opportunities. As one author points out: ‘many activities fall into a grey area between risks and opportunities – the Internet afford, indeed, risky opportunities’.<sup>28</sup>

For this reason, we also encourage the SALRC to draw a clearer distinction between risk and harm, as the potential prevalence or existence of online risks does not necessarily lead to experiences of harm.<sup>29</sup> *Discussion Paper 149* frequently seems to conflate risk and harm – a problem that is fairly common in the field of children’s online risk<sup>30</sup> but that should be resolved before even considering developing policies to counter so-called ‘risk’. Mere exposure to certain content does not necessarily result in harm, but nevertheless the SALRC and respondents quoted in the *Paper* seem to frequently confuse the number of children exposed to online risk (which is measurable) with the (presumably) lower number of children who actually experience harm as a result of such exposure (less easy to measure).<sup>31</sup>

Without properly differentiating between risk and harm, efforts like those of the SALRC to address supposed harms can actually restrict children’s rights.<sup>32</sup> While protection and the mitigation of risk are important as far as marginalised communities are concerned, we respectfully argue that an empowering approach to children’s rights is even more important.<sup>33</sup> We cannot afford to focus solely on risk, or our children will be excluded from the opportunities that also accompany Internet use and future technologies – something which South Africa can ill afford.

### Executive Summary – para 7.1:

---

<sup>28</sup> Livingstone, 2014, *ibid*.

<sup>29</sup> Livingstone & Helsper, *ibid*; Haddon, L. & Livingstone, S. (2014) “The Relationship between Offline and Online Risks” In: von Feilitzen, C. & Stenersen, J., (eds.) *Young people, media and health: risks and rights*. The Clearinghouse Yearbook (2014). Goteborg: Nordicom.

<sup>30</sup> Livingstone, S. (2013) Online risk, harm and vulnerability: reflections on the evidence base for child Internet safety policy. *Journal of Communication Studies*, vol. 18 (35): 13-28.

<sup>31</sup> Livingstone, 2014, *ibid*.

<sup>32</sup> Livingstone, 2009, *ibid*.

<sup>33</sup> *ibid*.

In line with international developments, we agree with and commend the recommendation that the term 'child pornography' be substituted with the term 'child sexual abuse material'.

While we recognise the SALRC's reasoning for using the term 'material' (Chapter 1, para 1.6), we prefer the use of the word 'content' in line with international developments pertaining to platform liability and other forms of harmful content. The term 'material', it is submitted, could have other unintended, broader interpretations and meanings not suited for this context.

#### **Executive Summary – para 7.2:**

While we take note of the recommendation to revise the definition of 'child pornography' to include 'live displays, sequences of images and any of the listed conduct that could be used to advocate, advertise or promote a child for sexual purposes', we are concerned that in order to remain relevant and to avoid future redundancy, definitions should rather refrain from highlighting specific technologies.

Evolving technology like those facilitated by AI and the Internet of things (IoT), additive manufacturing and other technologies of the so-called Fourth Industrial Revolution (4IR) could, for instance, introduce new opportunities for child sexual exploitation. Definitions should therefore be broad enough to cover future content that amount to child sexual abuse.

And as noted, while we recognise the SALRC's reasoning for using the term 'material', we prefer the use of the word 'content' in line with international developments pertaining to platform liability and other forms of harmful content. The term 'material', it is submitted, could have other, unintended or broader interpretations.

#### **Executive Summary – para 7.4:**

We agree with and commend the notion that the *intention* of the creator of child sexual abuse content is irrelevant.

#### **Executive Summary – para 7.6:**

While we provisionally agree with the motivation for criminalising the exposure of children to harmful content, we believe the criminalisation of 'all acts of exposing children to...content not suitable for children, in whatever manner' is overly broad and could have unintended and harmful consequences. It would also limit the realisation of other human rights children are entitled to (like the right to information and the right to freedom of expression) in a manner that would arguably not meet the Constitutional threshold of being legitimate, necessary and proportional to the aim of the limitation. We also respectfully submit that the decision on what content is suitable or not suitable is too subjective to warrant criminalise all "acts of exposing" children to such content.

*“...all devices (new and second hand) be issued or returned to a default setting that blocks inappropriate content, with an opt-in possibility depending on proof of age of the buyer/user as being 18 and older. Giving effect to this recommendation will serve to protect the child and the provider...”*

We are particularly concerned about and strongly disagree with the proposal to require a default setting on devices. This provision is not only technologically determinist and immensely impractical from an implementation point of view, but wholly neglects children’s rights to participate and contribute to the information society. In ostensibly trying to protect children, it risks limiting children’s rights in a manner that would arguably fail to meet the Constitutional threshold of being legitimate, necessary and proportional to the aim of the limitation.

As noted, a primary focus on risks could cause more harm than benefit by limiting children’s opportunities. Indeed, a mandatory default setting risks unduly/disproportionately restricting children’s rights.<sup>34</sup> While protection and the mitigation of risk are important as far as marginalised communities are concerned, we respectfully argue that an empowering approach to children’s rights is crucial.<sup>35</sup> The SALRC needs to strike a better balance between efforts to increase opportunities for children and efforts to decrease risks. We cannot afford to solely focus on risk, or our children will be excluded from the opportunities that also accompany Internet use and future technologies – something which South Africa can ill afford.

We also encourage the SALRC to draw a clearer distinction between risk and harm, as the potential prevalence or existence of online risks does not necessarily lead to experiences of harm.<sup>36</sup> *Discussion Paper 149* frequently seems to conflate risk and harm – a problem that should be resolved before even considering developing policies to counter so-called ‘risk’. Mere exposure to certain content does not necessarily result in harm, but nevertheless the SALRC and respondents quoted in the *Paper* seem to frequently confuse the number of children exposed to online risk (which is measurable) with the (presumably) lower number of children who actually experience harm as a result of such exposure (less easy to measure).<sup>37</sup>

### **Executive Summary – para 7.7:**

RIA and APC commend the SALRC for differentiating between the *creation* and *distribution* of consensual self-generated child sexual abuse content. We are concerned, however, that clauses like ‘in certain circumstances’ and ‘to certain children’ are too broad, subjective, and vague to enable useful distinctions to be drawn and will result in policy uncertainty.

### **Executive Summary – para 7.9:**

---

<sup>34</sup> Livingstone, 2009, *ibid*.

<sup>35</sup> *ibid*.

<sup>36</sup> Livingstone & Helsper, 2013, *ibid*, Haddon & Livingstone, 2014, *ibid*.

<sup>37</sup> Livingstone, 2014, *ibid*.

We agree with the need for a provisional recommendation to compel ‘electronic communication service providers’ and financial institutions ‘that are aware that their systems or facilities are being used in the commission of an offence involving child sexual abuse content’ to report such offences.

We are concerned, however, that the term ‘electronic communication service providers’ is undefined and would exclude current or potential future technological platforms that might not fall within proposed categories.

We also submit that it would be useful, for policy certainty purposes, to define when an awareness of the commission of an offence can be reasonably imputed.

### **Executive Summary – para 7.11:**

RIA and APC commend the SALRC for recognising the need for developing a national response to child sexual exploitation and abuse (CSEA) ‘in close collaboration with relevant industry and organizations’. But we recommend not only a multidisciplinary approach, but a more encompassing collaborative or multistakeholder approach which will give not just different ministerial departments a role, but also the private sector, technical community, civil society, and users (including, crucially, children). We contend that as far as CSEA are concerned, and particularly the role of technology like the Internet in hosting or distributing such content, all relevant stakeholders should be consulted and should be invited to play a role in developing a national response.

As noted in the introduction of this submission, the Internet is a global network of networks which has no central authority and essentially remains non-hierarchical and decentralized;<sup>38</sup> making it a particularly difficult governance challenge. For similar reasons, developing a national response to CSEA when the Internet is involved as a medium is problematic and requires broad participation and collaboration for governance responses to be effective.

We argue that a collaborative, multistakeholder approach to developing a national response to CSEA could be useful in enabling a higher degree of openness, transparency, and the broad-based collaboration and equal participation of all those affected.<sup>39</sup> This includes children themselves. Besides sharing ideas and taking decisions, a core justification for supporting a multistakeholder approach is that such approaches lead to ‘better, more inclusive Internet governance’<sup>40</sup> that ‘enhance transparency’ and help decision-makers take into account diverse viewpoints in a way that can even help to deepen democracy.<sup>41</sup>

---

<sup>38</sup> Kleinwächter, 2014, *ibid.*

<sup>39</sup> World Bank, 2016, *ibid.*

<sup>40</sup> Esterhuysen, A. (2014) “Global Mechanisms to Support National and Regional Multistakeholderism.” In: Drake, W.J. & Price, M. (Eds.) (2014) *Beyond NETmundial: The Roadmap for Institutional Improvements to the Global Internet Governance Ecosystem*. Available at: [http://www.global.asc.upenn.edu/app/uploads/2014/08/BeyondNETmundial\\_FINAL.pdf](http://www.global.asc.upenn.edu/app/uploads/2014/08/BeyondNETmundial_FINAL.pdf).

<sup>41</sup> c.f. Van der Spuy, 2017, *bid.*

Along with the role of children in the information society, the demand for and value of multistakeholder participation in Internet governance was first explicitly expressed at the WSIS, which took place in two phases between 2003 and 2005.<sup>42</sup> Since WSIS, various international and multilateral organizations have endorsed the need for multistakeholder participation, including the Organization for Economic Cooperation and Development (OECD) in 2008 and 2011; UNESCO at a WSIS+10 Review event in 2014; the Council of Europe in 2009; the International Telecommunication Union (ITU) in 2010 and 2014; the G8 at Deauville in 2011; and the African Union in 2014. At the UN General Assembly's ten-year review of WSIS in 2015, the continued relevance of the notion of multistakeholder collaboration in Internet governance was confirmed, with the explicit addition of technical, academic and 'all other relevant stakeholders'.<sup>43</sup>

Lastly, as far as the SALRC's recommendation that the SAPS establish a victim identification data base linked to Interpol's Child Sexual Exploitation Image Database, further details should be made public about both how such database will be established and how proposed data sharing or 'linking' is proposed and how individuals will be protected from surveillance without just cause.

It is respectfully submitted that this recommendation needs to be more carefully construed in order to prevent the exploitation of data. African adults' and children's digital personas and data are already used to feed into, improve, and alter emerging technologies, often without their consent.<sup>44</sup> The collection and processing of massive amounts of personal data – including those related to victim identification – sometimes enable researchers, private and public sector organisations to infer not only African's faces,<sup>45</sup> but their movements, activities and behaviour. Using African children as data sources (with or without their informed consent) will have far-reaching disciplining, ethical, political and practical implications for the way children are or will be seen and treated by not only emerging technologies and the private sector often responsible for them, but also by our governments.<sup>46</sup>

### **Executive Summary – para 7.12:**

While RIA and APC acknowledge the need for data retention and preservation for reasonable evidentiary purposes, we reiterate our concern that data must be kept safely and justly. As noted in our response to paragraph 7.11, this recommendation needs to be more carefully construed in order to prevent the abuse of data. We also emphasise the need to ensure the anonymity of any potential victims, along with the importance of ensuring the safe custody of harmful content.

But we would also like to request that an exception be made for research in the public interest: anonymised content could be made available for researchers to better understand the incidence,

---

<sup>42</sup> CSTD/UNCTAD (2015) *Implementing WSIS Outcomes: A Ten-Year Review*. Geneva/New York: United Nations. Available at: [http://unctad.org/en/PublicationsLibrary/dtlstict2015d3\\_en.pdf](http://unctad.org/en/PublicationsLibrary/dtlstict2015d3_en.pdf).

<sup>43</sup> UNGA, 2015, *ibid*.

<sup>44</sup> Makulilo, A.B. (2016) (Ed.) *African Data Privacy Laws*. New York: Springer International Publishing.

<sup>45</sup> Hawkins, A. (2018) "Beijing's Big Brother Tech Needs African Faces." *Foreign Policy*. Available at: <https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/> (accessed February 2019).

<sup>46</sup> Taylor, L. (2017) What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society*, July–December 2017: 1–14.

design, prevalence and responses to online harms like those addressed by *Discussion Paper 149*. This exception is important because one of the most significant policy challenges in curtailing potential risks that accompany children's (and adults') digital inclusion is the lack of data pertaining to how children access and use the Internet, including their preferences, needs, perceptions and experiences. Without gathering such data, our policymakers will remain unable to design effective policy responses to protect and promote children's rights online.

### **Draft Amendment Bill – preamble**

As noted, while we recognise the SALRC's reasoning for using the term 'material', we prefer the use of the word 'content' in line with international developments pertaining to platform liability and other forms of harmful content.

### **Draft Amendment Bill – sec 2. (a)**

In line with international developments, we agree with and commend the recommendation that the term 'child pornography' be substituted with the term 'child sexual abuse material'.

While we recognise the SALRC's reasoning for using the term 'material' (Chapter 1, para 1.6), we prefer the use of the word 'content' in line with international developments pertaining to platform liability and other forms of harmful content. The term 'material', it is submitted, could have other unintended, broader interpretations and meanings not suited for this context.

### **Draft Amendment Bill – sec 2. (b)**

We are concerned that the term 'inappropriate' in the context of 'adult sexual content' is too broad, subjective, and vague to enable useful distinctions to be drawn and will result in policy uncertainty.

### **Section (3)(a)(i):**

We commend the principle of the extension of protections to the mentally disabled. We believe however, that the amendments of the law aimed at protecting disabled people from harm should not undermine their human rights. Section 3(a)(i) proposes an amendment to the Index to the Criminal Law (Sexual Offences and Related Matters) Amendment Act of 2007, which would make it an offence to expose mentally disabled people to pornography. This amendment may be well-intended to extend protection against sexual grooming and abuse to mentally disabled people.

Mentally disabled people are also sexual beings, however, and should have the same sexual rights (dependent on context) which includes the right to explore their sexuality, to sexual and reproductive health, and to sexual experiences and sexual enjoyment. The proposed amendment would effectively make 'exposure' of pornography (as in making erotic content available to them to allow them to enjoy their sexual rights) to disabled people an offence. This could impact on caregivers and family members

of mentally disabled adults who exercise their sexual rights through accessing erotic material online. Furthermore, the term 'mentally' disabled refers to a wide range of disabilities and conditions entailing a wide range of different vulnerabilities, including vulnerability to sexual abuse. There are mentally disabled people who are able to have sexual experiences without being harmed, and for many, pornography (when legal and with consent) is a safe option.

While we therefore commend the underlying principle of the amendment, we are concerned about the wording of the amendment. More research needs to be done on the harms faced by mentally disabled people online, and more research needs to be done on the diversity of conditions falling under the term and how they affect mentally disabled people's vulnerability to abuse, as well as abilities to exercise their sexual rights.

**Draft Amendment Bill – sec 3. (b) (iii) (re 19B of Criminal Law (Sexual Offences and Related Matter Amendment Act, 2007))**

The term 'Misleading techniques on the internet' should be defined as it is too vague to enable sufficient policy certainty.

**Draft Amendment Bill – sec 3. (b) (iii)**

We submit that the use of the term 'persons who are mentally disabled' risks conflating children's capacities with those of people who are mentally disabled. These categories of users are likely to have very different needs and will react differently to potential online risks when it comes to sexual content, and should therefore not be conflated.

**Draft Amendment Bill – sec 4. (a) (i) (re sec 1 of Criminal Law (Sexual Offences and Related Matter Amendment Act, 2007))**

While we take note of the recommendation to revise the definition of 'child pornography' to include 'live displays, sequences of images and any of the listed conduct that could be used to advocate, advertise or promote a child for sexual purposes', we are concerned that in order to remain relevant and to avoid future redundancy, definitions should rather refrain from highlighting specific technologies.

As noted, evolving technology like those facilitated by AI, additive manufacturing and other technologies of the 4IR could, for instance, introduce new opportunities for child sexual exploitation. Definitions should therefore be broad enough to cover future content that amount to child sexual abuse. Further, while we recognise the SALRC's reasoning for using the term 'material', we prefer the use of the word 'content' in line with international developments pertaining to platform liability and other forms of harmful content.

**Draft Amendment Bill – sec 4. c) (iv) (re sec 19A of Criminal Law (Sexual Offences and Related Matter Amendment Act, 2007))**

A key concern raised is the proposed insertion of Section 19A **“Enticement to view or making child sexual abuse material or pornography accessible to children”**. Paragraph 2(a) of this amendment would make it an offence for a “person”, “manufacturer”, “distributor of any technology or device”, or an “electronic communications service provider” to “engage with any form of technology or device, including a mobile phone, that is capable of accessing the internet, social media, or other digital content, without ensuring that the default settings block access to child sexual abuse content or pornography, is guilty of an offence of making child sexual abuse content or pornography accessible to a child”.

Our concerns with the proposed section are both technical as well as related to the rights of children, parents, care givers, and (other) Internet users. They include that the implementation of Section 2(a) would have significant implications for access to and participation in the Internet in South Africa. While the wording of the 2(a) would make it an offense to provide child sexual abuse material as well as pornography to a child, we focus in the below on the significance of 2(a) making it an offence to make *pornography accessible to children* only. We agree that children should be protected from the harms posed by pornography and that it should be an offence to use pornography in the abuse, harm, or grooming of a child. Further research needs to be done on how to best protect children from the harms of pornography, whether children of all ages including teenagers and youth should be completely prevented from accessing pornography, as well as how to mitigate the harms caused by children inevitably (whether legally or not) accessing pornography.

Assuming, however, that it is agreed that *all* children should not be able to access pornography, and that it be made an offence to provide a device or connection through which a child may be able to access pornography, concerns remain. These include important questions about how to define what content comprises pornography and of how to implement the blocking of access of children to pornography effectively without blocking access to other benign or non-harmful content.

Section 2(a) could severely inhibit a child’s ability to access and use the Internet. It may be far easier for device manufacturers and connection providers to simply not make their devices or connections accessible to children than tackle the very hard technical as well as ethical and rights-based questions involved in implementing such a provision.

On a technical level, there are a number of ways of implementing 2(a), most of which may have very significant chilling effects on access to the Internet for children as well as adults. In accordance with its wording, section 2(a) would need to be implemented at the device and software level, as well as at the network level.

At the device and software level, new devices – including out of the box phones, computers, and laptops – would need to have customised software installed that detects and blocks pornography. This would require a significant effort. Every version of the Mac or Windows Operating system, or of Android for mobile phones, for example, would need to have aftermarket functionality integrated into the

software as well as, perhaps, in the device. Section 2(a) does not address how it could be practically implemented. Mobile operators, device manufacturers, and software developers would either have to consent to their devices being sold with after-market software or cooperate with and integrate the demands of 2(a). Assuming such cooperation could actually be attained, the extent of software development or patching actually required to implement the blocking of content on all devices in South Africa would require a large amount of time, labour, and resources that could prove to be a significant bottleneck to the supply chain of devices, software and services in the country. It is doubtful that the country will be able to implement pornography blocking on all devices without decreasing the supply and increasing the price of such devices.

Section 2(a) would also have to be implemented at a network level by electronic communications service providers. Electronic service providers like mobile phone operators and Internet service providers would be required to set-up filtering, blocking, and traffic analysis infrastructure and essentially provide two tiers of Internet access, one for adults and one for children, as well as authentication mechanisms to verify users. How this could successfully be implemented without introducing barriers to and increasing the prices of access has not been addressed by the SALRC. The Bill also leaves too much policy uncertainty as to how pornography and child sexual abuse material would be detected, and who would maintain such databases required to block content (like block lists) or software required to detect such content.

We are also concerned about paragraphs 2(b) and 2(c) of the proposed Section 19A. Paragraph 2(b) states that a person “who uninstalls the default setting blocking access to child sexual abuse material, is guilty of the offence of making child sexual abuse material accessible, 2(c) states that a person “who uninstalls the default setting blocking access to pornography without valid identification proving that the requester is a user over the age of 18, is guilty of an offence of making pornography accessible to a child”. These provisions apply to manufacturers or distributors of “any technology or device” as well as to electronic communications service providers and individual persons.

In addition to the technological implications of implementing such a system (dealt with above), the proposed amendments have significant implications for the personal computing freedom of adult persons. If all devices were to be issued with software that includes default settings blocking access to certain sites, and if the user needed to present identification to uninstall such software, it would mean that all software would need to be approved and modified by the law presumably through a state or state mandated authority. In order to uninstall some components of this software, individual persons would have to prove their age, while other components of the software would be illegal to uninstall regardless of the purpose. This would effectively amount to software mandated by a state authority and would infringe individuals’ privacy rights.

In order to enforce the law, all software distribution channels would likely need to be approved and modified by a state authority. In addition to needing buy-in from major software vendors, the provision would be almost impossible to implement as software could still be bought or downloaded online.

Without buy-in from major software vendors, access to the software repositories of Microsoft, Apple, Google, etc. would have to be blocked in South Africa.

There is also the question of Free and Open Source Software (FOSS), which encompasses software made available without charge by a developer community, much of which (e.g. the Linux operating system and the Apache web server software) is essential for the functioning of the modern Internet. The rigidly controlled software distribution channels proposed by the Bill would make much open source software illegal if it was not approved for use. A large amount, if not all, free software distribution channels would also need to be blocked in order to enforce the measures envisaged in the proposed Section 19A.

In addition to stifling individual software usage, innovation and the digital economy would be severely restricted if all software allowing access to the Internet needed to be pre-approved. Start-ups would have a very limited choice of software with which to run their businesses as well as to assemble their online infrastructures. In addition to being impractical to implement, section 19A would therefore inhibit individual and organisational software choice and usage as well as inhibit innovation in the digital economy.

We therefore strongly disagree with the notion, summarised in this provision, that providing access to a device ‘without ensuring that the default setting blocks access to child sexual abuse material or pornography’ will result in harm and should therefore be criminalised. We also encourage the SALRC to draw a clearer distinction between risk and harm, as the potential prevalence or existence of online risks does not necessarily lead to experiences of harm.<sup>47</sup> Mere exposure to certain content does not necessarily result in harm, but nevertheless the provision seems to frequently confuse the number of children exposed to online risk via a device on which a default setting was not activated with the number of children who actually experience harm as a result of such potential exposure.<sup>48</sup>

This ‘default provision’ suggestion is therefore not only technologically determinist and impractical from an implementation point of view, but wholly neglects not only children’s rights but adults’ rights too. As noted, a primary focus on risks could cause more harm than benefit by limiting children’s and adults’ opportunities. Indeed, efforts like this proposal to ostensibly address potential harms can actually restrict rights.<sup>49</sup> While protection and the mitigation of risk are important as far as marginalised communities are concerned, we argue that an empowering approach to children’s rights to rights to participate and contribute to the information society are even more important.<sup>50</sup> The SALRC needs to strike a better balance between efforts to increase opportunities for children and efforts to decrease risks.<sup>51</sup> We cannot afford to solely focus on risk, or our children (and adults, in this case) will be excluded from the opportunities that also accompany Internet use and future technologies.

---

<sup>47</sup>Livingstone & Helsper, 2013, *ibid*; Haddon & Livingstone, 2014, *ibid*.

<sup>48</sup>Livingstone, 2014, *ibid*.

<sup>49</sup>Livingstone, S. (2009) Maximising opportunities and minimising risks for children online: from evidence to policy. *Intermedia*, vol. 37 (4): 50-53.

<sup>50</sup>*ibid*.

<sup>51</sup>Livingstone & Helsper, 2013, *ibid*; Haddon & Livingstone, 2014, *ibid*.

**Draft Amendment Bill – sec 4. c) (iv) (re sec 19B of Criminal Law (Sexual Offences and Related Matter) Amendment Act, 2007))**

We submit that ‘misleading techniques on the Internet’ is poorly defined and still so poorly understood that the SALRC cannot propose criminalising it.

As noted, there is a lack of reliable data pertaining to how children younger than 15 years of age access and use the Internet, including the way they react to potential ‘misleading techniques’. Without understanding these practices, our policymakers are unable to make assumptions about children’s preferences, needs, risks, perceptions, and experiences. We submit that it is problematic and disconcerting that, despite this lack of data, assumptions are nevertheless made about how so-called ‘misleading techniques’ might harm children. While the possibility of harm through the exposure to pornographic content online exists, children’s susceptibility to be waylaid by ‘misleading techniques’ is too vaguely defined and not sufficiently backed up by evidence for the practice to be criminalised.

**Chapter 1, para 1.2:**

While we understand the SALRC’s focus on the ‘negative outcomes or risks associated with the use of ICT’s (*sic*) on the lives of children’, we caution that the positive and empowering potential of digital inclusion should not be neglected.

As noted, while the protection and the mitigation of risk are important as far as marginalised communities are concerned, we argue that an empowering approach to children’s rights to rights to participate and contribute to the information society are even more important.<sup>52</sup> The SALRC needs to strike a better balance between efforts to increase opportunities for children and efforts to decrease risks, although the two are closely related.<sup>53</sup> We cannot afford to focus solely on risk, or our children will be excluded from the opportunities that also accompany Internet use and future technologies – something which South Africa can ill afford.

We also encourage the SALRC to draw a clearer distinction between risk and harm, as the potential prevalence or existence of online risks does not necessarily lead to experiences of harm.<sup>54</sup> *Discussion Paper 149* frequently conflates risk and harm – a problem that should be resolved before even considering developing policies to counter so-called ‘risk’. Mere exposure to certain content does not necessarily result in harm, but nevertheless the SALRC and respondents quoted in the *Paper* seem to frequently confuse the number of children exposed to online risk (which is measurable) with the

---

<sup>52</sup> *ibid.*

<sup>53</sup> Livingstone, S.; Hasebrink, U. & Görzig, A. (2012) “Towards a general model of determinants of risk and safety” In: Livingstone, S.; Haddon, L & Görzig, A., (eds.) *Children, Risk and Safety on the Internet: Research and Policy Challenges in Comparative Perspective*. Bristol: Policy Pres

<sup>54</sup> Livingstone & Helsper, 2013, *ibid*; Haddon & Livingstone, 2014, *ibid.*

(presumably) lower number of children who actually experience harm as a result of such exposure (less easy to measure).<sup>55</sup>

### Chapter 1, para 1.7:

We would like to emphasise that with the exception of RIA's work, there is a lack of reliable data in general on ICT access and use in South Africa, including evidence regarding which children are more susceptible to potential risk or harm.

RIA's nationally-representative ICT access and use surveys referenced earlier in this submission<sup>56</sup> form part of a survey of 20 countries in the global South (ten of which are in Africa) that canvasses barriers to access from those not connected, as well as the challenges to optimal Internet usage even where there is coverage or the individual has connectivity. The in-depth questionnaire used seeks to identify the demand-side constraints on Internet access and particularly use. Traditional ICT indicators, fixed line, mobile phone, voice services and data are collected, as well as diverse areas of focus like:

- gender inequality in access and use;
- affordability and user strategies to access services, including zero-rated services, social media use, the use of free public Wi-Fi, and community networks;
- barriers to use, including affordability, skills, relevant content, language, and literacy;
- use of public information and government services online;
- mobile money and online transactions;
- cybersecurity and online rights awareness, including perceptions of trust, freedom of expression, privacy, surveillance; and (among other things)
- the extent and nature of microwork.

As it draws on the national census frame for sampling purposes, RIA's surveys cover 15 year-olds and older. Within the dataset, we have further categorised two youth groups (one from 15 to 18; another from 18 to 25) for our youth analysis. The survey therefore gathers no data on children below the age of 15 years (other than their presence in the household). We therefore agree with the UNCRC Committee that besides RIA's data on 15 year-olds and older, there is a lack of reliable data pertaining to how children younger than 15 years of age access and use the Internet, including their preferences, needs, perceptions and experiences. Without gathering such data, our policymakers are unable to make assumptions about children's preferences, needs, risks, perceptions, and experiences.

We submit that it is problematic and disconcerting that, despite this clear lack of data, assumptions are nevertheless made in *Discussion Paper 149* about risks, needs and experiences (e.g., para 2.2).

---

<sup>55</sup> Livingstone, 2014, *ibid*.

<sup>56</sup> Gillwald, Mothobi & Rademan, 2019, *ibid*.

While the likelihood of harm through the exposure to pornographic content online might be high, harm and risk need to be thoroughly understood in order to design and target policy interventions at those users (including children) who might be more susceptible or vulnerable of risk.

As noted, the SALRC must draw a clearer distinction between risk and harm, as the potential prevalence or existence of online risks does not necessarily lead to experiences of harm.<sup>57</sup> *Discussion Paper 149* frequently conflates these concepts – a problem that is fairly common in the field of children’s online risk<sup>58</sup> but that should be resolved before even considering developing policies to counter so-called ‘risk’. Mere exposure to certain content does not necessarily result in harm, but nevertheless the SALRC and respondents quoted in the *Paper* seem to confuse the number of children exposed to online risk (which is measurable) frequently with the (presumably) lower number of children who actually experience harm as a result of such exposure (less easy to measure).<sup>59</sup> Our policymakers should not make generic assumptions about children’s preferences, needs, perceptions and experiences – and should also not base policies or legislation on such assumptions.

### Chapter 1, para 1.16

In line with international developments, RIA and APC endorse and commend the recommendation that the term ‘child pornography’ be substituted with the term ‘child sexual abuse material’, although we would use the word ‘content’ rather than ‘material’. We prefer the use of the word ‘content’ in line with international developments pertaining to platform liability and other forms of harmful content.

### Chapter 2, para 2.1

We note the SALRC’s recommendation that ‘content providers’ should ‘take greater responsibility for the conscious targeting of children’, but note that the term ‘content provider’ is not defined in *Discussion Paper 149* and should be defined in a flexible manner.

It is further submitted that, in order to prevent the stifling of innovation and competition in global online markets,<sup>60</sup> the SALRC should consider differentiating between the size of a provider or platform, the nature of the platform (e.g., platforms that merely host content, platforms that actively create content, or platforms that moderate or curate content), and platforms’ or providers’ related obligations. While all businesses have the responsibility to protect and respect human rights regardless of their size, sector, operational context, ownership and structure, larger content providers or platforms arguably have different levels of responsibility. The scale and complexity of the means through which platforms

---

<sup>57</sup> Livingstone & Helsper, 2013, *ibid*; Haddon & Livingstone, 2014, *ibid*.

<sup>58</sup> Livingstone, 2013, *ibid*.

<sup>59</sup> Livingstone, 2014, *ibid*.

<sup>60</sup> Internet Society (2019) *Global Internet Report: Consolidation in the Internet Economy*. Geneva: ISOC. Available at: <https://future.internetsociety.org/2019/>.

or providers meet responsibilities, for instance, may vary according to these factors and with the severity of the platform or provider's potential impact on human rights.<sup>61</sup>

## Chapter 2, para 2.2

The contention that 'the internet has had the unintended consequence that children can access or be exposed to pornography in a manner that is unrestricted by legal and social constraints that govern such access and exposure in the "real" world' is problematic for at least two reasons.

First, the binary distinction between 'offline' and 'online' experience is flawed, as online and offline experiences are closely related and interlinked.<sup>62</sup> The effects of varied human rights infringements online echo, extend into and mingle with offline contexts,<sup>63</sup> and unsurprisingly have roots in offline realities and norms.<sup>64</sup> The distinction that tends to be drawn between offline and online dimensions is unproductive as many rights violations tend to occur in 'hybrid contexts of techno-mediated life, in the unfreedoms wrought by data, digitalisation and networks'.<sup>65</sup>

An unhelpful distinction between offline and online dimensions has often restricted users' agency and enabled more violations of their economic, social and cultural rights because there are no binding legal mechanisms by which such violations can be challenged effectively.<sup>66</sup> The use of the binary distinction between 'offline' and 'online' can also have other implications for the protection and mitigation of rights violations. For example, women (and likely also children) tend to underreport online infringements of human rights because 'victims' often believe online harms are too abstract to be taken seriously by relevant authorities, or that harms on social media platforms like Facebook or Twitter<sup>67</sup> are not equally serious than or on par with the harms that result from 'offline' infringements.

Second, the Internet does not facilitate 'harm' in a manner that is 'unrestricted by legal and social constraints' that apply in 'offline' contexts. While the Internet (and other ICTs) might enable relative anonymity (to a certain extent) and facilitates the sharing and distribution of content in novel ways, this does not mean the Internet is a 'law-free zone'.<sup>68</sup> The ways in which the Internet is designed has both allowed and disallowed specific types of behaviour online.<sup>69</sup> Although some have argued that the

---

<sup>61</sup> OHCHR (2011). Guiding Principles on Business and Human Rights. Available at: [https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR\\_EN.pdf](https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf).

<sup>62</sup> Van der Spuy & Aavriti, 2018, *ibid*.

<sup>63</sup> Dad & Khan, 2017, *ibid*; Digital Rights Foundation, 2016, *ibid*; Pasricha, 2016, *ibid*.

<sup>64</sup> Shephard, 2016, *ibid*.

<sup>65</sup> Gurumurthy & Chami, 2017, *ibid*.

<sup>66</sup> *ibid*.

<sup>67</sup> Chair, C. (2016, February 23) Women @ Facebook Roundtable: Discussing tech-related violence and solutions by African women. *The RIA Rap* (blog). Available at: [www.goo.gl/gU2UQj](http://www.goo.gl/gU2UQj); Kovacs, A., Richa, K. & Shobha, SV. (2013, April) "Don't let it stand!" *An Exploratory Study of Women and Verbal Online Abuse in India*. Internet Democracy Project. New Delhi: Internet Democracy Project. Available at: [www.internetdemocracy.in/wp-content/uploads/2013/12/Internet-Democracy-Project-Women-and-Online-Abuse.pdf](http://www.internetdemocracy.in/wp-content/uploads/2013/12/Internet-Democracy-Project-Women-and-Online-Abuse.pdf).

<sup>68</sup> Van der Spuy, 2017.

<sup>69</sup> Weiss, T.G. (2008) "Foreword." In Mathiason, J. (2009), *Internet Governance: The new frontier of global institutions*. Oxon: Routledge, xiii- xvi.

Internet is free from any regulatory oversight<sup>70</sup> or jurisdictional restraints<sup>71</sup> and should remain so, the Internet was never a different universe with separate, external legal constraints, though enforcement may present particular challenges.

We furthermore find the paragraph's contention that 'children are being harmed' and that the 'effect of pornography on children' is 'reported as wide ranging' problematic. As we have noted, one of the most significant policy challenges in curtailing potential risks that accompany children's (and adults') digital inclusion is the lack of data pertaining to how children access and use the Internet, including their preferences, needs, perceptions and experiences. Without gathering such data, our policymakers are unable to make generic assumptions about children's preferences, needs, perceptions and experiences.

As also noted, we encourage the SALRC to draw a clearer distinction between risk and harm, as the potential prevalence or existence of online risks does not necessarily lead to experiences of harm.<sup>72</sup> The paragraph conflates risk and harm – a problem that is fairly common in the field of children's online risk<sup>73</sup> but that should be resolved before even considering developing policies to counter so-called 'risk'. Mere exposure to certain content does not necessarily result in harm.<sup>74</sup>

## Chapter 2, para 2.18

*"A number of respondents affirm the view that exposure of children to pornography on the internet is problematic..."*

The statement should be unpacked. While a study of 'more than 1500 High school children' in Gauteng is referenced, no explanation is provided for how the sample was selected and what the evidentiary value of the study is.

As mentioned, one of the most significant policy challenges in curtailing potential risks that accompany children's (and adults') digital inclusion is the lack of data pertaining to how children access and use the Internet, including their preferences, needs, concerns, perceptions and experiences. Without gathering such data, our policymakers are unable to make assumptions about children's concerns, preferences, needs, perceptions and experiences. And they are even less able to develop policies on the basis of such assumptions of children's concerns, preferences, needs, perceptions and experiences.

---

<sup>70</sup> Barlow, J.P. (1996, February 8). *A Declaration of the Independence of Cyberspace*. Davos, Switzerland.

<sup>71</sup> e.g., Johnson, D.R. & Post, D.G. (1996). Law and Borders – The Rise of Law in Cyberspace, *Stanford Law Review*, 48(5): 1367-1402; *Yahoo Inc. v. LICRA* 433 F.3d 1199 (9th Cir. 2006).

<sup>72</sup> Livingstone & Helsper, 2013, *ibid*; Haddon & Livingstone, 2014, *ibid*.

<sup>73</sup> Livingstone, 2013, *ibid*.

<sup>74</sup> Livingstone, 2014, *ibid*.

As noted, we encourage the SALRC to draw a clearer distinction between risk and harm, as the potential prevalence or existence of online risks does not necessarily lead to experiences of harm.<sup>75</sup> Mere exposure to certain content does not necessarily result in harm, but nevertheless the SALRC and respondents quoted in the *Paper* seem to frequently confuse the number of children exposed to online risk (which is measurable) with the (presumably) lower number of children who actually experience harm as a result of such exposure (less easy to measure).<sup>76</sup>

## Chapter 2, para 2.19

*“Some respondents submit that although exposure to pornography is problematic, it has always been a problem and cannot be attributed to the advent or expansion of access to the internet alone.”*

Again, we warn that the SALRC must differentiate between exposure to potentially harmful content and actual outcomes of risk. The fact that a child is exposed to pornography or other potentially harmful content does not necessarily mean she or he will experience harm – and as such, such exposure cannot be deemed *per se* problematic or harmful.

We again encourage the SALRC to draw a clearer distinction between risk and harm, as the potential prevalence or existence of online risks does not necessarily lead to experiences of harm.<sup>77</sup> *Discussion Paper 149* frequently seems to conflate risk and harm – a problem that is fairly common in the field of children’s online risk<sup>78</sup> but that should be resolved before even considering developing policies to counter so-called ‘risk’. Mere exposure to certain content does not necessarily result in harm, but nevertheless the SALRC and respondents quoted in the *Paper* seem to frequently confuse the number of children exposed to online risk (which is measurable) with the (presumably) lower number of children who actually experience harm as a result of such exposure (less easy to measure).<sup>79</sup>

We would also like to encourage the SALRC to delve deeper into the nuance between experiences with exposure to pornographic content online and offline in the context of the phrase. As mentioned, the binary distinction between ‘offline’ and ‘online’ experience is problematic, as online and offline experiences are closely related and interlinked.<sup>80</sup> The effects of varied human rights infringements online echo, extend into and mingle with offline contexts,<sup>81</sup> and unsurprisingly have roots in offline realities and norms.<sup>82</sup> An unhelpful distinction between offline and online dimensions has often restricted users’ agency and enabled more violations of their economic, social and cultural rights because there is no binding legal mechanisms by which such violations can be challenged effectively.<sup>83</sup>

---

<sup>75</sup> Livingstone & Helsper, 2013, *ibid*; Haddon & Livingstone, 2014, *ibid*.

<sup>76</sup> Livingstone, 2014, *ibid*.

<sup>77</sup> Livingstone & Helsper, 2013, *ibid*; Haddon & Livingstone, 2014, *ibid*.

<sup>78</sup> Livingstone, 2013, *ibid*.

<sup>79</sup> Livingstone, 2014, *ibid*.

<sup>80</sup> Van der Spuy & Aavriti, 2018, *ibid*.

<sup>81</sup> Dad & Khan, 2017, *ibid*; Digital Rights Foundation, 2016, *ibid*; Pasricha, 2016, *ibid*.

<sup>82</sup> Shephard, 2016, *ibid*.

<sup>83</sup> *ibid*.

*“According to some respondents further contributing factors are that almost every child has access to a mobile phone, iPad, tablet, laptop or computer and children can accidentally or deliberately log onto sites; parents are not cyber smart and do not know about filters and blocking of sites...”*

This claim needs to be further examined with reference to existing or new nationally-representative data on how children and adults use the Internet. As we have noted, one of the most significant policy challenges in curtailing potential risks that accompany children’s (and adults’) digital inclusion is the lack of data pertaining to how children access and use the Internet, including their preferences, needs, perceptions and experiences. Without gathering such data, our policymakers are unable to make assumptions or develop evidence-based policies to address problems.

RIA’s surveys have shown that only 53% of South Africans above the age of 15 years have access to the Internet. Anecdotally, we assume that many children and people who are yet to come online are likely to be the poorest in society and therefore more vulnerable and susceptible to risk as they often tend to lack the necessary digital literacy skills to know how to ameliorate risks when they do eventually gain Internet access. There is a lack of reliable data pertaining to how children younger than 15 years of age access and use the Internet, including their preferences, needs, perceptions and experiences. Without gathering such data, our policymakers are unable to make assumptions about children’s preferences, needs, perceptions, and experiences. And they are even less able to develop policies on the basis of such assumptions of children’s concerns, preferences, needs, perceptions and experiences.

Risk must be studied and better understood. *Discussion Paper 149* frequently conflates risk and harm – a problem that is fairly common in the field of children’s online risk<sup>84</sup> but that should be resolved before even considering developing policies to counter so-called ‘risk’. Mere exposure to certain content does not necessarily result in harm, but nevertheless the SALRC and respondents quoted in the *Paper* seem to frequently confuse the number of children exposed to online risk (which is measurable) with the (presumably) lower number of children who actually experience harm as a result of such exposure (less easy to measure).<sup>85</sup>

## **Chapter 2, para 2.20**

We note the SALRC’s recommendation that ‘content providers’ are ‘clearly not doing enough’, but point out that it would be helpful to summarise what ‘content providers’ are doing at the moment in making such a claim and assessment – including the various mechanisms social media platforms like Facebook or Twitter have implemented in this regard, and the efficacy thereof.

We also repeat that the term ‘content provider’ is not defined in *Discussion Paper 149* and should be defined in a flexible manner. To prevent the stifling of innovation and competition in global online

---

<sup>84</sup> Livingstone, 2013, *ibid.*

<sup>85</sup> Livingstone, 2014, *ibid.*

markets,<sup>86</sup> the SALRC should consider differentiating between the size of a provider or platform, the nature of the platform (e.g., platforms that merely host content, platforms that actively create content, or platforms that moderate or curate content), and platforms' or providers' related obligations. While all businesses have the responsibility to protect and respect human rights regardless of their size, sector, operational context, ownership and structure, larger content providers or platforms arguably have different levels of responsibility. The scale and complexity of the means through which platforms or providers meet responsibilities, for instance, may vary according to these factors and with the severity of the platform or provider's potential impact on human rights.<sup>87</sup>

## Chapter 2, para 2.26

*“Respondents are of the view that children are being exposed to a range of pornography including adult pornography, self-generated sexual material between peers and child sexual abuse material...”*

As mentioned, one of the most significant policy challenges in curtailing potential risks that accompany children's (and adults') digital inclusion is the lack of data pertaining to how children access and use the Internet, including their preferences, needs, concerns, perceptions and experiences. Without gathering such data, our policymakers are unable to make generic assumptions about children's concerns, preferences, needs, perceptions and experiences.

We caution that exposure to 'a range of pornography' does not necessarily lead to harm, and that before developing regulatory responses to a perceived harm, harm should be shown. We encourage the SALRC to draw a clearer distinction between risk and harm, as the potential prevalence or existence of online risks does not necessarily lead to experiences of harm.<sup>88</sup>

A primary focus on risks could cause more harm than good by limiting children's opportunities. While protection and the mitigation of risk are important as far as marginalised communities are concerned, we respectfully argue that an empowering approach to children's rights to participate and contribute to the information society are even more important.<sup>89</sup> The SALRC needs to strike a better balance between efforts to increase opportunities for children and efforts to decrease risks.<sup>90</sup>

## Chapter 2, para 2.26

The section lists causes for children's exposure to pornography, including 'easy internet access'. As explained above, South Africa lacks data to claim that we have 'easy internet access'. While anecdotally we know that some children gain Internet access at schools even if their parents do not have access, RIA's nationally-representative data of South Africans aged 15 years and above indicate

---

<sup>86</sup> Internet Society, 2019, *ibid*.

<sup>87</sup> OHCHR (2011). Guiding Principles on Business and Human Rights. Available at: [https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR\\_EN.pdf](https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf).

<sup>88</sup> Livingstone & Helsper, 2013, *ibid*; Haddon & Livingstone, 2014, *ibid*.

<sup>89</sup> *ibid*.

<sup>90</sup> Livingstone, Hasebrink & Görzig, 2012, *ibid*.

that only 53% of South Africans have access to the Internet – and same can often not be described as ‘easy’. For those who are online, Internet use is often brief and passive. Only a limited number of South Africans are known to have the skills or resources to participate meaningfully online.<sup>91</sup>

### Chapter 2, para 2.30

The paragraph mentions ‘more vulnerable children’ and the fact that not all children react to harmful content in the same manner – that ‘the reaction is dependent on factors relating to the child’s background and social and moral modeling’.

We are firstly concerned about the use of the term ‘modeling’ in this context (which could refer to morals) and submit that a more neutral term such as ‘socialization’ is more nuanced. The assertion is otherwise crucial to other claims of risk and harm in *Discussion Paper 149* and needs to be further examined with reference to existing or new data. Factors like socioeconomic stratification, regulatory frameworks, technological infrastructure and a country’s education system have been recognised as important factors that impact how children experience online risk and whether it translates to harms.<sup>92</sup> High Internet use tends to be associated with higher risks (but not necessarily harm). Interestingly, children in countries with higher GDPs tend to encounter more online risks, although such countries may also be better placed to develop adequate responses and safety resources.<sup>93</sup> While much research and policymaking tends to talk about children in general, very little work has been done to differentiate and identify children who are more susceptible or vulnerable to risk beyond demographic factors. This leads to ‘a tendency to recommend blanket policies for all children which are too restrictive for many and yet still insufficient for some’.<sup>94</sup>

### Chapter 2, para 2.32

*“This sparks interest as children who are naturally curious are lured to view age inappropriate explicit content. This increases their risk of becoming victims of criminals who seek to target and abuse children for commercial gain.”*

This assertion needs to be further examined with reference to existing or new data. As mentioned, much research and policymaking tends to talk about children in general while very little work has been done to differentiate and identify children who are more susceptible or vulnerable to risk beyond demographic factors. This leads to ‘a tendency to recommend blanket policies for all children which are too restrictive for many and yet still insufficient for some’.<sup>95</sup>

---

<sup>91</sup> Gillwald, Mothobi & Rademan, 2019, *ibid.*

<sup>92</sup> Livingstone, Hasebrink & Görzig, 2012, *ibid.*

<sup>93</sup> *ibid.*

<sup>94</sup> Livingstone, 2009, *ibid.*

<sup>95</sup> *ibid.*

Factors like socioeconomic stratification, regulatory frameworks, technological infrastructure and a country's education system have been recognised as important factors that impact how children experience online risk and whether it translates to harms.<sup>96</sup> High Internet use tends to be associated with higher risks (but not necessarily harm). Interestingly, children in countries with higher GDPs tend to encounter more online risks, although such countries may also be better placed to develop adequate responses and safety resources.<sup>97</sup>

### Chapter 2, para 2.37

*"While a range of views and personal experiences were shared on what the effects of exposing children to pornography are, the common response was that the effects on children are all negative. ... The effects of exposing a child to pornography which have been identified by all of the respondents point to a negative and sometimes life impacting change in the child's behaviour which in turn can affect future life choices and behaviour..."*

We again stress that it cannot be assumed that the effects of exposing children to pornography are *per se* negative without evidence and data to that effect. A clearer distinction must be drawn between risk and harm, as the potential prevalence or existence of online risks does not necessarily lead to experiences of harm.<sup>98</sup> This section again seems to conflate risk and harm – a problem that should be resolved before even considering developing policies to counter so-called 'risk'. Mere exposure to certain content does not necessarily result in harm.<sup>99</sup>

We also caution that the positive and empowering potential of digital inclusion and Internet use should not be neglected. A primary focus on risks could cause more harm than benefit by limiting children's opportunities. While protection and the mitigation of risk are important as far as marginalised communities are concerned, we argue that an empowering approach to children's rights to participate and contribute to the information society are even more important.<sup>100</sup> The SALRC therefore needs to strike a better balance between efforts to increase opportunities for children and efforts to decrease risks.<sup>101</sup> We cannot afford to focus solely on risk. If we do so, South African children will be excluded from the opportunities that also accompany Internet use and future technologies – something which the country cannot afford.

### Chapter 2, para 2.50

*...the focus should be on education of children, parents, teachers and caregivers regarding what pornography is, what the harms are, what constitutes a healthy sexual relationship, how to respond to peer pressure and how to put in place measures to protect children against grooming.*

---

<sup>96</sup> Livingstone; Hasebrink & Görzig, 2012; *ibid.*

<sup>97</sup> *ibid.*

<sup>98</sup> Livingstone & Helsper, 2013, *ibid.*; Haddon & Livingstone, 2014, *ibid.*

<sup>99</sup> Livingstone, 2014, *ibid.*

<sup>100</sup> *ibid.*

<sup>101</sup> Livingstone, Hasebrink & Görzig, 2012, *ibid.*

We agree that an empowering approach, which includes a focus on education and digital literacy, are crucial.

### Chapter 2, para 2.52

*Some respondents suggest that the solution to protecting children from exposure would be to make the default position that all pornography is unavailable on the internet. To access it adults would have to pay an extra fee or specifically subscribe to it... the NPA in turn submits that internet access and social media should be limited for children. Pornography access should be regulated by paid sites only, and finger print access should be implemented and be compulsory.*

Our concerns with the default proposal are both rights-based and technical. Implementation of proposed default options would have significant implications for access to and participation in the Internet by people living in South Africa. We agree that children should be protected from the potential harms posed by pornography and that it should be an offence to use pornography in the abuse, harm, or grooming of a child. But further research needs to be done on how to best protect children, and for children to protect themselves from the harms of pornography, whether children of all ages including teenagers and youth should be completely prevented from accessing pornography, as well as how to mitigate the harms caused by children inevitably (whether legally or not) accessing pornography.

Assuming, however, that it is agreed that *all* children should not be able to access pornography, and that it be made an offence to provide a device or connection through which a child may be able to access pornography, concerns remain. These include important questions about how to define what content comprises pornography and of how to implement the blocking of access of children to pornography effectively without blocking access to other benign or non-harmful content. It may be far easier for device manufacturers and connection providers to simply not make their devices or connections accessible to children than tackle the very hard technical as well as ethical and rights-based questions involved in implementing such a provision.

We also encourage the SALRC to draw a clearer distinction between risk and harm, as the potential prevalence or existence of online risks does not necessarily lead to experiences of harm.<sup>102</sup> Mere exposure to certain content does not necessarily result in harm, but nevertheless the provision seems to frequently confuse the number of children exposed to online risk via a device on which a default setting was not activated with the number of children who actually experience harm as a result of such potential exposure.<sup>103</sup>

This 'default provision' suggestion is therefore not only technologically determinist and impractical from an implementation point of view, but wholly neglects children's and adults' rights. As noted, a primary

---

<sup>102</sup> Livingstone & Helsper, 2013, *ibid*; Haddon & Livingstone, 2014, *ibid*.

<sup>103</sup> Livingstone, 2014, *ibid*.

focus on risks could cause more harm than benefit by limiting children's and adults' opportunities. Indeed, efforts like this proposal to ostensibly address potential harms can actually restrict rights.<sup>104</sup> While protection and the mitigation of risk are important as far as marginalised communities are concerned, we argue that an empowering approach to children's rights is even more important.<sup>105</sup> The SALRC needs to strike a better balance between efforts to increase opportunities for children and efforts to decrease risks.<sup>106</sup> We cannot afford to solely focus on risk, or our children (and adults, in this case) will be excluded from the opportunities that also accompany Internet use and future technologies.

### Chapter 2, para 2.52

*"...Children should be taught about the principles of the use of social media and ICT's, the risks, dangers and unacceptable use of the ICT" (sic)*

We agree that an empowering approach, which includes a focus on how to safely and responsibly use social media and ICTs, is crucial.

### Chapter 2, para 2.52

*"...in the South African context where some children are being raised by grandparents who have no idea of the technology and its consequences, service providers are obliged to be fully engaged in combating exposure to pornography..."*

While it may be true that some children may be more susceptible to risk, the assertion must be further examined with reference to existing or new data. As mentioned, factors like socioeconomic stratification, regulatory frameworks, technological infrastructure and a country's education system have been recognised as important factors that impact how children experience online risk and whether it translates to harms.<sup>107</sup> High Internet use tends to be associated with higher risks (but not necessarily harm). Interestingly, children in countries with higher GDPs tend to encounter more online risks, although such countries may also be better placed to develop adequate responses and safety resources.<sup>108</sup> While much research and policymaking tends to talk about children in general, very little work has been done to differentiate and identify children who are more susceptible or vulnerable to risk beyond demographic factors. This leads to 'a tendency to recommend blanket policies for all children which are too restrictive for many and yet still insufficient for some'.<sup>109</sup>

Not only does the term 'service providers' have to be defined, but we believe further detail should be provided about what obligations are actually being proposed. As mentioned, if an obligation is

---

<sup>104</sup> Livingstone, 2009, *ibid.*

<sup>105</sup> *ibid.*

<sup>106</sup> Livingstone & Helsper, 2013, *ibid*; Haddon & Livingstone, 2014, *ibid.*

<sup>107</sup> Livingstone, Hasebrink & Görzig, 2012, *ibid.*

<sup>108</sup> *ibid.*

<sup>109</sup> Livingstone, 2009, *ibid.*

proposed as far as providers are concerned, the SALRC should consider differentiating between the size of a provider or platform, the nature of the platform (e.g., platforms that merely host content, platforms that actively create content, or platforms that moderate or curate content), and platforms' or providers' related obligations. While all businesses have the responsibility to protect and respect human rights regardless of their size, sector, operational context, ownership and structure, larger content providers or platforms arguably have different levels of responsibility. The scale and complexity of the means through which platforms or providers meet responsibilities, for instance, may vary according to these factors and with the severity of the platform or provider's potential impact on human rights.<sup>110</sup>

*"...suggests that software should be embedded in phones to prevent any and all access to pornographic sites. It contends that while some may feel this impinges on their right of access to information this needs to be balanced against the best interests of the child."*

We strongly disagree with this suggestion. The suggestion to 'embed' software is not only technologically determinist and immensely impractical from an implementation point of view, but wholly neglects children's rights to participate and contribute to the information society. As noted, a primary focus on risks could cause more harm than benefit by limiting children's and adults' opportunities. Indeed, efforts like those of the SALRC to address supposed risks can actually restrict rights.<sup>111</sup> While protection and the mitigation of risk is important, we respectfully argue that an empowering approach is even more important.<sup>112</sup> The SALRC needs to strike a better balance between efforts to increase opportunities for children and efforts to decrease risks, although the two are closely related.<sup>113</sup> We cannot afford to solely focus on risk, or South African children (and adults, in this case) will be excluded from the opportunities that also accompany Internet use and future technologies.

We also encourage the SALRC to draw a clearer distinction between risk and harm, as the potential prevalence or existence of online risks does not necessarily lead to experiences of harm.<sup>114</sup> Mere exposure to certain content does not necessarily result in harm, but nevertheless the SALRC and respondents quoted in the *Paper* seem to frequently confuse the number of children exposed to online risk (which is measurable) with the (presumably) lower number of children who actually experience harm as a result of such exposure (less easy to measure).<sup>115</sup>

## Chapter 2, para 2.111

*"...the need to take into account the practical and technical considerations of implementing a uniform classification system in respect of online content."*

---

<sup>110</sup> OHCHR (2011). Guiding Principles on Business and Human Rights. Available at: [https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR\\_EN.pdf](https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf).

<sup>111</sup> *ibid.*

<sup>112</sup> *ibid.*

<sup>113</sup> Livingstone, Hasebrink & Görzig, 2012, *ibid.*

<sup>114</sup> Livingstone & Helsper, 2013, *ibid*; Haddon & Livingstone, 2014, *ibid.*

<sup>115</sup> Livingstone, 2014, *ibid.*

We agree with the submission and note that a uniform classification system for online content is not only impractical from an implementation point of view, but neglects children's rights to participate and contribute to the information society.

### Chapter 2, para 2.112

*"...it is not technically feasible for content distributors to submit all their content to anybody for pre-classification before publication, without interfering with the dynamic nature of the Open Web."*

We agree and note that a pre-publication classification for online content is not only immensely impractical from an implementation point of view, but will amount to a significant infringement of the right to freedom of expression and neglects children's rights to participate and contribute to the information society.

### Chapter 2, para 2.118

*"...children are not merely victims; they are experts on their own behaviour; what places them at risk; how they should act to protect themselves and how to contribute to the safety of their peers."*

We strongly agree with Media Monitoring Africa (MMA) in this regard and note that children's agency should not be neglected. Mere exposure to certain content does not necessarily result in harm, but nevertheless the SALRC and respondents quoted in the *Paper* seem to frequently conflate the number of children exposed to online risk with the number of children who actually experience harm as a result of such exposure.<sup>116</sup>

Similarly, not all children who are exposed to risk become victims. As noted, factors like socioeconomic stratification, regulatory frameworks, technological infrastructure and a country's education system have been recognised as important factors that impact how children experience online risk and whether it translates to harms.<sup>117</sup> High Internet use tends to be associated with higher risks (but not necessarily harm). Interestingly, children in countries with higher GDPs tend to encounter more online risks, although such countries may also be better placed to develop adequate responses and safety resources.<sup>118</sup> While much research and policymaking tend to talk about children in general, very little work has been done to differentiate and identify children who are more susceptible or vulnerable to risk beyond demographic factors. This leads to 'a tendency to recommend blanket policies for all children which are too restrictive for many and yet still insufficient for some'.<sup>119</sup>

---

<sup>116</sup> *ibid.*

<sup>117</sup> Livingstone, Hasebrink & Görzig, 2012, *ibid.*

<sup>118</sup> *ibid.*

<sup>119</sup> Livingstone, 2009, *ibid.*

*“...It advises that external protection in a form of filters needs to be developed in partnership with children in light of their own concerns and experiences in using the online environment...”*

We strongly agree with MMA in this regard and note that children should be involved, alongside all other stakeholders with a legitimate interest in the development of any regulatory response (including filters), including the private sector, technical community, civil society, and other users (including children). As noted in the introduction of this submission, the Internet has no central authority and essentially remains non-hierarchical and decentralized;<sup>120</sup> making it a particularly difficult governance challenge. For similar reasons, developing a national response to CSEA when the Internet is involved as a medium is problematic and requires broad participation and collaboration for governance responses to be effective.

A collaborative, multistakeholder approach to developing a national response to CSEA could be useful in enabling a higher degree of openness, transparency, and the broad-based collaboration and equal participation of those affected<sup>121</sup> (including children). Besides sharing ideas and taking decisions, one core justification for supporting a multistakeholder approach is that such approaches lead to ‘better, more inclusive Internet governance’<sup>122</sup> that ‘enhance transparency’ and help decision-makers take into account diverse viewpoints in a way that can even help to deepen democracy.<sup>123</sup>

*“...It further states that policy and legislation is not enough to address the issue of access, and exposure to pornography. In this regard MMA advocates for digital literacy as a key component to the protection of children.”*

We strongly agree with Media Monitoring Africa that an empowering approach to children’s rights, which includes a focus on education and digital literacy, are crucial.

## **Chapter 2, para 2.130**

*“...caution that in respect of accessing content and contact, ignoring the reality that some children engage in risky online conduct themselves and are therefore not always innocent roleplayers or bystanders, is to the detriment of children.”*

We strongly agree with the contention in the submission and note that children’s agency should not be neglected. Mere exposure to certain content does not necessarily result in harm, but nevertheless the SALRC and respondents quoted in the *Paper* seem to frequently conflate the number of children exposed to online risk with the lower number of children who actually experience harm as a result of such exposure.<sup>124</sup>

---

<sup>120</sup> Kleinwächter, 2014, *ibid.*

<sup>121</sup> World Bank, 2016, *ibid.*

<sup>122</sup> Esterhuysen, 2014, *ibid.*

<sup>123</sup> Van der Spuy, 2017.

<sup>124</sup> Livingstone, 2014, *ibid.*

As noted, not all children who are exposed to risk become victims. Factors like socioeconomic stratification, regulatory frameworks, technological infrastructure and a country's education system have been recognised as important factors that impact how children experience online risk and whether it translates to harms.<sup>125</sup> High Internet use tends to be associated with higher risks (but not necessarily harm). Children in countries with higher GDPs tend to encounter more online risks, although such countries may also be better placed to develop adequate responses and safety resources.<sup>126</sup> While much research and policymaking tend to talk about children in general, very little work has been done to differentiate and identify children who are more susceptible or vulnerable to risk beyond demographic factors.<sup>127</sup>

### Chapter 2, para 2.160

*"Most respondents link exposure to pornography and the objectification of the female and child body to a rise in sexual attacks and a number of negative outcomes..."*

We respectfully disagree with the notion that exposure to pornography *per se* leads to certain negative consequences or other 'negative outcomes'. We encourage the SALRC to draw a clearer distinction between risk and harm, as the potential prevalence or existence of online risks does not necessarily lead to experiences of harm.<sup>128</sup>

### Chapter 2, para 2.161

*"The Commission is of the view that while seeking to protect children from exposure to pornography it should be acknowledged that children are sexual beings albeit not sexually knowledgeable beings." (original emphasis)*

We strongly believe children should be enabled and entrusted to develop their knowledge in a safe and secure manner, and that simply withholding knowledge from them is not a reasonable or empowering response. We caution that the positive and empowering potential of digital inclusion and Internet use should not be subordinated to assumed harms, just because children might not be 'sexually knowledgeable beings'.

As noted, while the protection and mitigation of risk are important as far as marginalised communities are concerned, we respectfully argue that an empowering approach to children's which includes a focus on education and digital literacy, even more important.<sup>129</sup> The SALRC needs to strike a better balance between efforts to increase opportunities for children and efforts to decrease risks, although

---

<sup>125</sup> Livingstone, Hasebrink & Görzig, 2012, *ibid*.

<sup>126</sup> *ibid*.

<sup>127</sup> Livingstone, 2009, *ibid*.

<sup>128</sup> Livingstone & Helsper, 2013, *ibid*; Haddon & Livingstone, 2014, *ibid*.

<sup>129</sup> *ibid*.

the two are closely related.<sup>130</sup> We cannot afford to focus solely on risk, or our children will be excluded from the opportunities that also accompany Internet use and future technologies – something which South Africa can ill afford.

*“...Amidst the growing concern for the wellbeing of children it is however necessary to voice a word of caution in respect of the numerous quotes pertaining to statistics. Unfortunately not all statistics in this often hidden area of the law are supported by science. In fact it is posited that crime statistics do not measure the incidence of crime, but rather measure the reporting behaviour of victims... Consequently it is important to guard against speculation and at times exaggeration in order to make the situation appear more ghastly than it is. Having said this, conservative statistics from other countries in respect of exposure to pornography and an increase in adolescent sex offenders and an increase in sexual assaults perpetrated by young children are similar in South Africa and fairly consistent.”*

We strongly agree with the need to evaluate the statistics and sources used to infer experiences of harm carefully, or ‘to guard against speculation’, and warn that adopting even conservative statistics from other contexts (especially those in the global North, from where most available data is derived) will not enable local policymakers to make any reasonable inferences about the potential consequences of exposure to pornography.

As we have noted, one of the most significant policy challenges in curtailing potential risks that accompany children’s (and adults’) digital inclusion is the lack of data pertaining to how children access and use the Internet, including their preferences, needs, perceptions and experiences. Without gathering such data, our policymakers are unable to make generic assumptions about children’s preferences, needs, perceptions and experiences. We emphasise that it is neither sufficient nor acceptable to base policy recommendations on even ‘conservative statistics’ from other contexts.

RIA’s surveys have shown that only 53% of South Africans above the age of 15 years have access to the Internet. We know from the household data that many children and people who are yet to come online are likely to be the poorest in society and therefore more vulnerable and susceptible to risk as they often tend to lack the necessary digital literacy skills to know how to ameliorate risks when they do eventually gain Internet access. But there is a lack of reliable data pertaining to how children younger than 15 years of age access and use the Internet, including their preferences, needs, perceptions and experiences. Without gathering such data, our policymakers are unable to make reasonable assumptions about children’s preferences, needs, perceptions, and experiences.

Risk must be studied and better understood. *Discussion Paper 149* frequently conflates risk and harm, but mere exposure to certain content does not necessarily result in harm.<sup>131</sup>

---

<sup>130</sup> Livingstone, Hasebrink & Görzig, 2012, *ibid*.

<sup>131</sup> Livingstone, 2014, *ibid*.

## Chapter 2, para 2.166

*“South Africa is reported to have relatively high levels of ICT use for the region. 70% of youth aged 9 – 17 access the internet mostly through mobile phone telephony, with half of those having access whenever they wanted.”*

While it is true that South Africa has relatively high levels of ICT use for the region, the country compares poorly with better comparator countries in Latin America that have similar size economies and populations, though not as extreme inequalities. It would be useful if the statistics quoted would be referenced to enable a better understanding of methodologies and samples used. As noted, RIA’s surveys have shown that only 53% of South Africans above the age of 15 years have access to the Internet. There is a lack of reliable data pertaining to how children younger than 15 years of age access and use the Internet, including their preferences, needs, perceptions and experiences. The statistics also argue that a significant proportion ‘have access whenever they wanted’. As noted, RIA research shows that for the 53% of South Africans above the age of 15 years who are online, Internet use is often brief and passive. Only a limited number of South Africans have the skills or resources to participate meaningfully online.<sup>132</sup>

Without gathering better data, or explaining the sources of the data that do exist, our policymakers are unable to make generic assumptions about children’s preferences, needs, perceptions, and experiences. And they are even less able to design effective policy responses to potential risks.

## Chapter 2, para 2.166

*“The Commission agrees with the view that safety initiatives and messages irrespective of the platform should be available in South Africa in all official languages and not only English.”*

We support the notion that messages or legal content should, as far as is reasonably possible for platforms, be available in countries’ official languages. As noted, nine of South Africa’s eleven official languages are underrepresented online. English and Afrikaans remain the only languages with a strong online presence on news websites and platforms.<sup>133</sup> The lack of relevant content in users’ home language is a significant barrier to meaningful Internet access and use.<sup>134</sup>

That said, we believe that the SALRC can only propose translations as far as they are reasonably possible. It is important to prevent the stifling of innovation and encourage competition in global online markets.<sup>135</sup> Considering the fact that translations to *all* of South Africa’s official languages might be prohibitively expensive for especially smaller competitors, the SALRC should consider differentiating between the size of a provider or platform, the nature of the platform (e.g., platforms that merely host

---

<sup>132</sup> Gillwald, Mothobi & Rademan, 2019, *ibid*.

<sup>133</sup> Freedom House, 2018, *ibid*.

<sup>134</sup> Gillwald, Mothobi & Rademan, 2019, *ibid*.

<sup>135</sup> Internet Society, 2019, *ibid*.

content, platforms that actively create content, or platforms that moderate or curate content), and platforms' or providers' related obligations. While all businesses have the responsibility to protect and respect human rights regardless of their size, sector, operational context, ownership and structure, larger content providers or platforms arguably have different levels of responsibility. The scale and complexity of the means through which platforms or providers meet responsibilities, for instance, may vary according to these factors and with the severity of the platform or provider's potential impact on human rights.<sup>136</sup>

## Chapter 2, para 2.170

*"The Commission agrees that there is a real need for an in-depth understanding of the nature of technology including internet technology and how it is used to abuse and exploit children in South Africa..."*

RIA and APC commend the Commission for agreeing that there is a 'real need' for better understanding technology and its potential risks. But we caution that while understanding risk is vital, the positive and empowering potential of digital inclusion and Internet use should not be neglected. Efforts like those of the SALRC to understand Internet technology and 'how it is used to abuse and exploit children in South Africa' can actually restrict children's rights<sup>137</sup> by limiting children's opportunities. While protection and the mitigation of risk are important as far as marginalised communities are concerned, we respectfully argue that an empowering approach to children's rights is even more important.<sup>138</sup> The SALRC needs to strike a better balance between efforts to increase opportunities for children and efforts to decrease risks, although the two are closely related.<sup>139</sup>

*"The Commission is mindful that the development of modern ICT's and the media is largely controlled by the private sector... the question should be posed as to how it is necessary in the offline world to have statutory protection, but in the online world self-regulation will do?"*

Current trends in especially the Internet economy tend towards consolidation across and within the access, services and applications layer of the Internet, and regulators are still struggling to ascertain how to best deal with the impact of consolidation on society and economic development.<sup>140</sup>

But the SALRC's suggestion that 'the offline world' is somehow different or distinct from 'the online world', or that it is only subject to self-regulation, is problematic. The same rights we have offline also apply online. While online governance is more complex, it is far from impossible. Furthermore, as noted, the effects of varied human rights infringements online echo, extend into and mingle with offline

---

<sup>136</sup> OHCHR (2011). Guiding Principles on Business and Human Rights. Available at: [https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR\\_EN.pdf](https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf).

<sup>137</sup> Livingstone, 2009, *ibid*.

<sup>138</sup> *ibid*.

<sup>139</sup> Livingstone, Hasebrink & Görzig, 2012, *ibid*.

<sup>140</sup> Internet Society, 2019, *ibid*; Moore, M. & Tambini, D. (Eds.) (2018) *Digital Dominance: The Power of Google, Amazon, Facebook*. Oxford: Oxford University Press; Wu, T. (2018) *The Curse of Bigness: Antitrust in the New Gilded Age*. Columbia Global Reports.

contexts,<sup>141</sup> and unsurprisingly have roots in offline realities and norms.<sup>142</sup> The distinction that tends to be drawn between offline and online dimensions is unproductive as many rights violations tend to occur in 'hybrid contexts of techno-mediated life, in the unfreedoms wrought by data, digitalisation and networks'.<sup>143</sup>

## Chapter 2, para 2.171

*"...establish close working partnerships between law enforcement authorities and the ICT industry and internet and wireless application service providers by way of a memorandum of understanding."*

RIA and APC commend the SALRC's recognition of the need for close working relationship between law enforcement authorities, the 'ICT industry', and 'internet and wireless application service providers', but encourage it to consider adopting a broader collaborative or multistakeholder approach which will give not just different some stakeholders a role, but any interested party from the private sector, technical community, civil society, and users (including children). We feel that all relevant stakeholders should be consulted and should be invited to play a role in developing national responses to child online protection.

A collaborative, multistakeholder approach to developing a national response to CSEA could be useful in enabling a higher degree of openness, transparency, and the broad-based collaboration and equal participation of those affected.<sup>144</sup> This includes children. Besides sharing ideas and taking decisions, one core justification for supporting a multistakeholder approach is that such approaches lead to 'better, more inclusive Internet governance'<sup>145</sup> that 'enhance transparency' and help decision-makers take into account diverse viewpoints in a way that can even help to deepen democracy.<sup>146</sup>

## Chapter 2, para 2.175

*"...The view is further held that users are consciously targeted with the aim of developing addiction and online behaviour which may be habit forming. The point is to get online users 'through the door' in very much the same way as tobacco and alcohol advertising."*

While we commend the SALRC for taking note of the potential of online content and other tools to influence behaviour in various ways that might be habit-forming, we note that this is an issue that relates to online content as a whole and not merely content that relates to potential child online abuse. As such, while we recognise the importance of the issue, we contend that it falls outside the scope of the SALRC's work in *Discussion Paper 149*.

---

<sup>141</sup> Dad & Khan, 2017, *ibid*; Digital Rights Foundation, 2016, *ibid*; Pasricha, 2016, *ibid*.

<sup>142</sup> Shephard, 2016, *ibid*.

<sup>143</sup> Gurumurthy & Chami, 2017, *ibid*.

<sup>144</sup> World Bank, 2016, *ibid*.

<sup>145</sup> Esterhuysen, 2014, *ibid*.

<sup>146</sup> c.f. Van der Spuy, 2017.

That said, it is important to note global developments to address a variety of online harms which include the impact of technology on behaviour, democracy, children, attention and relationships.<sup>147</sup> The UK, for instance, is currently consulting on its so-called *Online Harms White Paper*.<sup>148</sup> While not without criticism and flaws, the *White Paper* points out that no country has yet been able to address online harms in a single or coherent way.

*“The view is therefore held that these companies need to take a greater responsibility for the conscious targeting of children.”*

We again commend the SALRC for recognising the role companies may play in the ‘conscious targeting of children’, but note that the practice is still poorly understood due to the limited amount of data and literature available on the incidence and prevalence of micro targeting – especially in an emerging country context like South Africa. It is both dangerous and impractical to compel ‘companies’ to ‘take greater responsibility’ for something which the extent and consequences of which are poorly understood.

Besides the need for further evidence and research to understand the consequences of micro targeting before developing policy responses thereto, it is further submitted that, in order to prevent the stifling of innovation and competition in global online markets, the SALRC should consider differentiating between the size of a provider or platform, the nature of the platform (e.g., platforms that merely host content, platforms that actively create content, or platforms that moderate or curate content), and platforms’ or providers’ related obligations. While all businesses have the responsibility to protect and respect human rights regardless of their size, sector, operational context, ownership and structure, larger content providers or platforms arguably have different levels of responsibility. The scale and complexity of the means through which platforms or providers meet responsibilities, for instance, may vary according to these factors and with the severity of the platform or provider’s potential impact on human rights.<sup>149</sup>

#### Chapter 4, para 4.198

*“...Users of these platforms are no longer satisfied that these global businesses are sidestepping protecting user’s rights on their platforms... Although platform owners have required user reporting before acting, Facebook has already demonstrated that it has an algorithm to remove naked images...”*

While it is true that algorithms or artificial intelligence can be used in some instances to filter and remove images automatically, the example listed also shows that it is often flawed and unable to read the contexts or potential public interest or historical value of certain images or content. Where nudity is concerned, for instance, cultural values play a significant role in dictating what is deemed acceptable

---

<sup>147</sup> See, for example, the work of the Center for Humane Technology: <https://ledger.humanetech.com>.

<sup>148</sup> HM Government, 2019, *ibid*.

<sup>149</sup> OHCHR (2011). Guiding Principles on Business and Human Rights. Available at: [https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR\\_EN.pdf](https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf).

or not in certain circumstances. The data used to train and implement such governance tools are often tested in a developed country context (primarily the global North, with data sets that often tend to belong to specific populations). If such tools are deployed, they must be improved to also 'read' other conditions better.

Some have already started doing so, however, in rather exploitative ways. Despite the low levels of Internet use in Africa, for instance, Africans' digital personas and data are being used to feed into, improve, and alter emerging technologies, and their privacy is therefore just as at risk as active data subjects in the Global North.<sup>150</sup> The collection and processing of massive amounts of personal data enable researchers, private and public sector organisations to infer not only African's faces,<sup>151</sup> but their movements, activities and behaviour. Using Africans as data sources (with or without their informed consent) have far-reaching disciplining, ethical, political and practical implications for the way people are or will be seen and treated by not only emerging technologies and the private sector often responsible for them, but also by African governments.<sup>152</sup>

On the other hand, such filtering tools only go so far. The Christchurch mosque attack of earlier 2019, for instance, was live streamed on Facebook. It was re-uploaded by other users after it was taken down by the company, and then shared on various other platforms and websites too. There may therefore be a need for a cross-sectoral, multinational collaboration or clearing house for emergency responses in certain instances. But because social media platforms are sometimes used to record and raise awareness of human rights violations (e.g., war crimes in Syria), content also cannot simply be deleted. It must be safely archived and kept for evidentiary and research purposes.<sup>153</sup>

#### Chapter 4, para 4.246

*"...children in wealthy private schools and in desperate poverty in the township of Alexandra face the same risks. He is however of the view that the response to a child who is involved in 'sexting' or becomes the victim of sexual coercion and extortion is however glaringly different depending on the status of the child, leaving vulnerable children at greater risk."*

This is an interesting suggestion that would need further examination before developing policy on the basis of its implications. The reasons why some children may be more vulnerable or susceptible to abuse or harm online, for instance, needs to be better understood, as blanket policies for all children may be insufficient for some whilst too restrictive for others. The suggestion that children in townships are poorly prepared to deal with risk does, however, seem to echo findings from studies done elsewhere: children in countries with higher GDPs tend to encounter more online risks, although such countries may also be better placed to develop adequate responses and safety resources.<sup>154</sup>

---

<sup>150</sup> Makulilo, 2016, *ibid.*

<sup>151</sup> Hawkins, 2018, *ibid.*

<sup>152</sup> Taylor, 2017, *ibid.*

<sup>153</sup> Van der Spuy, 2019, *ibid.*

<sup>154</sup> *ibid.*

As mentioned, much research and policymaking tends to talk about children in general while very little work has been done to differentiate and identify children who are more susceptible or vulnerable to risk beyond demographic factors. This leads to ‘a tendency to recommend blanket policies for all children which are too restrictive for many and yet still insufficient for some’.<sup>155</sup> Factors like socioeconomic stratification, regulatory frameworks, technological infrastructure and a country’s education system have been recognised as important factors that impact how children experience online risk and whether it translates to harms.

#### Chapter 4, para 4.247

*“Experts identified by the European Cybercrime Centre point out the following characteristics of children vulnerable to online sexual coercion and extortion:*

- *‘naivety of the victims, either on a relational level or on a technical level;*
- *Absence of parental control;*
- *Willingness to share self-generated sexual content;*
- *Significant amount of time spent online each day;*
- *Use of social networks and other ways of online communication, especially through mobile devices;*
- *Befriending strangers (unknowns);*
- *Sexualised conversations with strangers;*
- *Lack of technical knowledge.”*

Whilst these factors are certainly interesting, we still lack sufficient evidence to determine accurately which children in a South African context might be more susceptible or vulnerable to risk online. While it is unclear what the European Cybercrime Centre is basing its factors on, they are likely to refer to children in a very different European context which cannot be extrapolated to South Africa. As noted, blanket policies for all children may be insufficient for some whilst too restrictive for others.

As mentioned, much research and policymaking tends to talk about children in general while very little work has been done to differentiate and identify children who are more susceptible or vulnerable to risk beyond demographic factors. This leads to ‘a tendency to recommend blanket policies for all children which are too restrictive for many and yet still insufficient for some’.<sup>156</sup> Factors like socioeconomic stratification, regulatory frameworks, technological infrastructure and a country’s education system have been recognised as important factors that impact how children experience online risk and whether it translates to harms.

#### Chapter 4, para 4.255

---

<sup>155</sup> Livingstone, 2009, *ibid.*

<sup>156</sup> *ibid.*

*“The Commission is however mindful that legislative change alone would not be apposite to address this problem. The Commission is also of the view that no country would be able to prosecute itself out of this phenomenon. Different levels of intervention are necessary.”*

We agree with the contention that legislative change alone will not only be insufficient, but also impractical considering the practical difficulty of addressing especially online abuse and the pace of technological change. As noted, the Internet is a global network of networks which enables communication between networks using certain protocols to communicate across layers on a global and mostly public scale. Taken as a whole, the Internet has no central authority and essentially remains non-hierarchical and decentralized;<sup>157</sup> making it a particularly difficult governance challenge. For similar reasons, developing a national response to the problem where the Internet is involved as a medium is problematic and requires broad participation and collaboration for governance responses to be effective.

A collaborative, multistakeholder approach to developing a national response to the problem could be useful in enabling a higher degree of openness, transparency, and the broad-based collaboration and equal participation of those affected.<sup>158</sup> This includes children themselves. Besides sharing ideas and taking decisions, one core justification for supporting a multistakeholder approach is that such approaches lead to ‘better, more inclusive Internet governance’<sup>159</sup> that ‘enhance transparency’ and help decision-makers take into account diverse viewpoints in a way that can even help to deepen democracy.<sup>160</sup>

#### **Chapter 6, para 6.1**

*“...include the need to ensure anonymity of the child depicted in the child sexual abuse material in the criminal justice system; safe custody of child sexual abuse material; access to child sexual abuse material by the defence; data preservation; access by SAPS and suspension of access to child sexual abuse material by ECSPs...”*

While we agree with the need to ensure the anonymity of any potential victim(s), along with the importance of ensuring the safe custody of harmful content, we would also like to emphasise the importance of enabling access to such content for both research and evidentiary purposes.

We would therefore like to request that an exception be made for research in the public interest: anonymised content could be made available for researchers to better understand the incidence, design, prevalence and responses to online harms like those addressed by *Discussion Paper 149*.

#### **Chapter 6, para 6.47**

---

<sup>157</sup> Kleinwächter, 2014, *ibid.*

<sup>158</sup> World Bank, 2016, *ibid.*

<sup>159</sup> Esterhuysen, 2014, *ibid.*

<sup>160</sup> Van der Spuy, 2017, *ibid.*

*“From the outset there is a need for a clear and effective reporting and support mechanism for children, their caregivers, ECSP’s and any other concerned person with regard to these offences.”*

We agree with the suggestion that a ‘clear and effective reporting and support mechanism’ should be made available, but add that such a mechanism should, as far as is reasonably possible, also be available in different languages.

Where online content is concerned, it is important to note that perpetrators of abuse sometimes use multiple platforms to spread or distribute content to increase the impact thereof (e.g., WhatsApp, Facebook, Twitter, email programmes). While isolated bits of content on a single platform might not seem significantly harmful when viewed in isolation, when content from diverse platforms are viewed together in the context concerned (often amounting to a flood or deluge of content deployed with the aim of maximising discomfort or harm), it becomes more harmful. Therefore we also suggest that the SALRC consider online reporting mechanisms that could be platform agnostic or which could operate across online platforms to simplify reporting procedures for victims, and to enable quicker takedown of harmful content.

That said, we believe that the SALRC can only propose reporting mechanisms as far as they are reasonably possible. It is important to prevent the stifling of innovation and encourage competition in global online markets.<sup>161</sup> Considering the fact that the development and maintenance of adequate reporting mechanisms might be prohibitively expensive for especially smaller competitors, the SALRC should consider differentiating between the size of a provider or platform, the nature of the platform (e.g., platforms that merely host content, platforms that actively create content, or platforms that moderate or curate content), and platforms’ or providers’ related obligations. While all businesses have the responsibility to protect and respect human rights regardless of their size, sector, operational context, ownership and structure, larger content providers or platforms arguably have different levels of responsibility. The scale and complexity of the means through which platforms or providers meet responsibilities, for instance, may vary according to these factors and with the severity of the platform or provider’s potential impact on human rights.<sup>162</sup>

---

<sup>161</sup> Internet Society, 2019, *ibid*.

<sup>162</sup> OHCHR (2011). Guiding Principles on Business and Human Rights. Available at: [https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR\\_EN.pdf](https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf).