Suite No.2, Art Centre, 22 6th St, Parkhurst, Johannesburg, 2193
Tel: +27 11 78 1278 | Fax: + 27 11 788 1289 | Email: info@mma.org.za
www.mediamonitoringafrica.org

28 May 2025

TO: UNITED NATIONS OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS
E-mail: ohchr-privacy2025@un.org

SUBMISSION BY MEDIA MONITORING AFRICA:

CALL FOR INPUT ON THE RIGHT TO PRIVACY IN THE DIGITAL AGE

For more information, please contact:

William Bird, Director, Media Monitoring Africa
Email: williamb@mma.org.za
Tel: +27 11 788 1278

Thandi Smith, Head of Programmes, Media Monitoring Africa
Email: thandis@mma.org.za
Tel: +27 11 788 1278

Phakamile Madonsela, Public and Media Skills Manager, Media Monitoring Africa
Email: phakamilek@mma.org.za
Tel: +27 11 788 1278

INTRODUCTION

1. Media Monitoring Africa ("MMA") welcomes the opportunity to provide this submission to the United Nations Office of the High Commissioner for Human Rights ("High Commissioner") for its report on the challenges and risks regarding discrimination and the unequal enjoyment of the right to privacy associated with the collection and processing of data.

2. Privacy is both a standalone right and a foundational enabler of other rights, including freedom of expression, dignity, and autonomy. As such, the protection of privacy must be regarded as an essential pillar of broader human rights safeguards. The integration of artificial intelligence ("AI") on digital platforms presents both opportunities and challenges for the protection of privacy rights. The expansive data collection and processing required for AI tools has heightened security and transparency concerns, particularly for children, whose personal information is often gathered, analysed, and integrated into complex predictive models without their full understanding or consent.[1] Without adequate safeguards, AI-driven systems risk exacerbating existing inequalities, reinforcing discrimination, and perpetuating systemic biases that disproportionately impact vulnerable groups such as children.

3. This submission focuses on the implications of AI-driven data processing, particularly in relation to children's privacy rights, transparency, and digital governance. In assessing these issues, this submission draws on research conducted by MMA on children in South Africa and offers regional comparative perspectives to highlight privacy and transparency concerns emanating from the collection and processing of data online.

4. As such, and in line with our expertise, we structure our submission as follows:

    4.1. ***First,*** we examine how AI-driven data collection and processing affects children's privacy rights.

    4.2. ***Second,*** we review MMA's findings on the lack of clarity regarding data collection, storage, and usage, and demonstrate how this has impacted children's perspectives on digital privacy.

    4.3. ***Third,*** we provide an overview of measures to mitigate risks, including regulatory frameworks and accountability mechanisms.

    4.4. ***Lastly,*** we provide examples of good practices to enhance protection for vulnerable groups such as children.

OVERVIEW OF MEDIA MONITORING AFRICA

5. Established in 1993 as a not-for-profit organisation, MMA has been at the forefront of addressing the harms of disinformation and advocating for freedom of expression and

[1] Paul, 'Privacy and data security concerns in AI' (2024) (accessible here) at 1-2.

the responsible flow of information to the public.[2] In turn, MMA has implemented effective media strategies for impactful change by leveraging technology, social media, and data tools.

6. MMA's focus has also been on raising public awareness about children's rights and the importance of protecting their privacy on digital platforms. As such, MMA has engaged in several projects aimed at educating children, guardians, and educators on online safety, recognising gaps in online safety mechanisms for children, and empowering children to safeguard against exploitation and harm online. Additionally, MMA has grappled with the implementation and use of AI in online spaces, including its implementation and use on social media platforms.

7. Some notable projects include:

    7.1. Drafting several guidelines and discussion documents on AI usage and governance and engaging extensively with different stakeholders to promote the responsible use of AI on digital platforms.[3]

    7.2. The development of the Real411 which is a publicly accessible platform that enables members of the public to report concerns about online harms such as hate speech and disinformation.[4]

    7.3. The development of an online political advertisement repository, "PADRE", where political parties can upload their official ads.[5] This repository helps the media and public distinguish real ads from altered ones.[6]

    7.4. In 2024, MMA hosted a discussion around AI, disinformation, and election integrity at the Goethe-Institut and, in the same year, highlighted the impact of AI on journalism during its Media Freedom Festival.[7]

    7.5. In 2020, MMA made its submissions to the Committee on the Rights of the Child on the Draft General Comment on Children's Rights in Relation to the Digital Environment. In its submissions, MMA outlined the importance of critical digital

[2] For example, MMA has prepared several publications on disinformation and the right to freedom of expression during elections, the impact of disinformation on children and children's rights, and disinformation on climate change. These publications are available on MMA's website (here).
[3] See, for example, MMA, 'Guidelines for Media Organisations Using Generative AI'(2024) (accessible here); MMA, 'Guidelines for Political Parties Using Generative AI' (2023) (accessible here); Forum on Information & Democracy, 'Artificial Intelligence in the Information and Communications Space' (2023) (accessible here); MMA, 'Discussion document: The Implications of Artificial Intelligence on Information Rights' (2021) (accessible here).
[4] Real411 (accessible here); See also MMA, 'Final: Impact of Mis- and Disinformation in the 2024 National and Provincial Elections in South Africa' (2024) (accessible here); Bird & Smith, 'Real411 is ready to process your complaints about election misinformation and disinformation' *Daily Maverick* (2024) (accessible here); and Bird & Smith, 'Real411 develops new tool to track incitement on social media' *Daily Maverick* (2024) (accessible here) for more information on Real411.
[5] See website (here).
[6] Hawkins, 'Elections 2024: IEC ready to fend off deep fakes' *Bloemfontein Courant* (2024) (accessible here); MMA, 'Media Coverage and Disinformation in the run up to the elections' (14 September 2021) (accessible here).
[7] SANEF, '2024 Media Freedom Festival Tackles Journalism's Key Challenges' (21 October 2024) (accessible here).

literacy in ensuring children's meaningful engagement with the digital environment.[8]

7.6. In 2025, MMA launched its "Judicial Handbook for Navigating Online Harms" – a vital resource addressing online harassment, data protection, and privacy rights.[9]

7.7. MMA also developed and manages Insights into Incitement or i3, an AI model that detects incitement of violence on social media and other online platforms.[10] The platform provides insight into the levels of incitement online, with the view of informing strategies to address it.

8. For more information about MMA, please visit: mediamonitoringafrica.org.

IMPACT OF AI-DRIVEN DATA COLLECTION AND PROCESSING ON CHILDREN'S PRIVACY RIGHTS

9. South Africa and the African region at large continue to grapple with obstacles to achieving universal internet access, with disparities in connectivity limiting meaningful digital participation.[11] Unresolved issues related to data governance, privacy, and cybersecurity further complicate the responsible implementation of AI technologies. The region's existing legal frameworks remain inadequate to address AI's far-reaching economic, legal, political, and regulatory implications, both on- and offline.

10. A major concern is AI's role in data amplification, algorithmic bias, and privacy. AI-driven processes often reinforce existing biases in data sets, affecting automated decision-making and potentially furthering existing inequalities. nderstanding the intersectionality of children's identities becomes crucial to recognising unique vulnerabilities in AI-driven environments. For example, LGBTQI+ children may face unfair treatment due to biased algorithms that influence content moderation and data collection, potentially exposing them to discrimination or limiting their access to affirming spaces. Children with disabilities may struggle with accessibility challenges, as AI-driven interfaces often fail to accommodate diverse needs, such as automated consent mechanisms that do not adequately support different cognitive or physical abilities. Similarly, marginalised children, particularly in the Global South, encounter barriers to informed consent due to AI models being trained predominantly in English.

11. Additionally, AI can exacerbate online harms by facilitating the spread of disinformation and hate speech while enabling more sophisticated forms of digital harassment and violence which often disproportionately affect children. The regulation of online content has introduced additional layers of restriction as AI-driven moderation systems increasingly enforce community standards by automatically identifying and removing objectionable material, often with minimal human

[8] MMA, 'Submission to the Committee on the Rights of the Child on the Draft General Comment on Children's Rights in Relation to the Digital Environment' (2020) (accessible here). See also MMA, 'Children's Rights Online: Towards a Digital Rights Charter' (2020) (accessible here) at 19-20.
[9] MMA 'Judicial Handbook for Navigating Online Harms' (2025) (accessible here).
[10] See website (here).
[11] Mathekga, 'Bridging Africa's digital divide' (27 June 2024) (accessible here).

oversight.[12] For example, TikTok employs automated systems as its "first line of defense" in the sense that AI and machine learning technologies are leveraged to detect and flag harmful content automatically and serve as the initial filter by scanning content for clear violations.[13] Further, a range of issues and topics are already being blocked for children's engagement. While the filtering and removal of some content, such as content of an overt, explicit, or harmful nature like self-harm or child sexual abuse material ("CSAM") might be understandable, AI systems have also been used to block educational content on topics such as sexuality and reproductive rights. AI can thus serve as a cover for limiting and preventing children from engaging in a range of issues and subjects. As such, there is a need for AI systems to provide clarity, transparency, and accountability regarding what is included, moderated, and restricted. We cannot allow the same gaps, omissions, threats, and flaws currently in place on social media platforms to be simply replicated as this will only deepen existing digital divides.

12. Children also often struggle to grasp the implications of sharing personal information with digital systems. AI relies on vast amounts of data, including sensitive identifiers such as location and biometric information, raising concerns about consent, transparency, and accountability.[14] Children, particularly younger ones, may unwittingly disclose excessive personal information to AI interfaces, making them vulnerable to privacy breaches, security threats, and potential exploitation.[15] This issue is exacerbated by the digital divide, which disproportionately affects children from majority-world countries where the lack of digital infrastructure and legal protections reinforce existing socio-economic disparities thus making them more vulnerable to these harms.[16]

FINDINGS ON CHILDREN'S PERSPECTIVES ON DIGITAL PRIVACY

South Africa's Young People's Perspectives on Digital Privacy

13. In 2024, MMA published a research report entitled 'South Africa's Young People's Perspectives on Digital Privacy'.[17] The study examined young people's perspectives on privacy and trust in the digital age with consideration to their complex and evolving views on online data protection.[18] While the participants identified privacy as fundamental to autonomy, relationships, security, and personal boundaries, many were sceptical of the use of digital services.[19] This distrust stemmed from a lack of transparency, limited control over data, and concerns about algorithmic decision-making.[20]

---

[12] MMA, 'Discussion document: The Implications of Artificial Intelligence on Information Rights' (2021) (accessible here) at 13.
[13] TikTok, 'Transparency Centre' (accessible here).
[14] UNICEF, 'Policy guidance on AI for children' (2021) (accessible here) at 23.
[15] Id.
[16] UNICEF above n 16 at 23.
[17] MMA, 'South African Young People's Perspectives on Digital Privacy' (2024) (accessible here). The research was conducted through an in-person workshop with 24 children (aged 13 to 17) in Johannesburg and a broader survey of 60 more from across South Africa.
[18] Id at 3.
[19] MMA above n 19 at 3.
[20] Id.

14. The children outlined several recommendations that could potentially be used as policy protection principles. These include advocating for greater control over their data, stronger transparency measures, enhanced security protocols, and restrictions on data sharing and tracking.[21] They also emphasised the importance of automatic data deletion and minimal data collection, particularly for individuals under 18, to mitigate risks associated with excessive digital surveillance.[22]

Children-led technical research study

15. On 21 September 2024, the Article 12 Working Group, with support from MMA, conducted a child-led research project examining children's user experiences on TikTok and Instagram.[23] The study focused on five key aspects: the availability of languages for Terms of Service ("ToS"), default privacy settings, safety features, account deletion processes, and recommendations for improving children's privacy on these platforms.[24]

16. Findings revealed that TikTok and Instagram had limited language accessibility for South African users.[25] TikTok offered Kiswahili as its only African language and while Instagram included Afrikaans, it lacked broader regional representation.[26] Regarding default privacy settings, TikTok accounts for 17-year-olds were automatically set to "public", with no option to choose between "private" or "public" during setup.[27] Instagram required users to actively select privacy settings, but its design failed to emphasise the importance of enhanced privacy for minors.[28] Researchers noted that privacy explanations on Instagram could be simplified.

17. The study also highlighted inconsistencies in global privacy protections. Instagram had implemented stricter privacy policies for users under 18 in select regions like the United Kingdom, the United States of America, Canada, and Australia but these measures had not been extended to South African users.[29] Additionally, the study examined safety features such as privacy controls, two-step verification, device management, and security alerts. While it was found that these mechanisms help protect users, effective utilisation was seen to require a certain level of digital literacy, which not all children possessed.[30]

18. The study concluded with recommendations to improve children's experiences on these platforms. These recommendations included emphasising the need for expanded language accessibility, automatic privacy protections for users under 18,

[21] MMA above n 19 at 6.
[22] Id.
[23] The Article 12 Working Group acts as child online safety ambassadors for MMA. See MMA, 'Child-Led Technical Research Study Outline and Findings' (2024) (accessible here) at 1.
[24] Id.
[25] MMA above n 25 at 3.
[26] Id.
[27] MMA above n 25 at 3.
[28] MMA above n 25 at 4.
[29] Id.
[30] MMA above n 25 at 5-6.

clearer safety information, and a more balanced approach to parental oversight.[31] The recommendations also called for improved platform navigation.[32]

Comparative study: Young people, privacy and trust in Ghana

19. A comparative analysis of children's perceptions of privacy across Ghana and South Africa revealed common concerns regarding trust in digital platforms. In a study conducted on "Young people, privacy and trust in Ghana", Ghanaian children expressed ambivalence about their data security with many acknowledging that while they rely on online platforms in daily life, they remain sceptical about how their data is collected, used, and protected.[33] While some children cited strong security features and company reputations as reasons to trust certain platforms, others highlighted fears of surveillance, data breaches, and the misuse of personal information, especially for advertising purposes.[34] Concerns about tracking, unauthorised data sharing, and potential exploitation were also discussed.[35]

20. In their recommendations, the children emphasised the need for stronger security measures, including anti-virus systems and firewalls, to prevent unauthorised access.[36] They also asked for data minimisation and an end to excessive tracking, particularly for users under 18.[37] The participants also asked that platforms avoid selling or distributing their information without consent.[38] Control and transparency emerged as critical priorities, as many felt they lacked sufficient agency over how their data was used and wanted clearer explanations regarding data collection practices.[39]

REGULATORY FRAMEWORKS AND ACCOUNTABILITY MECHANISMS

21. Across the region, several countries have adopted legislation, policy frameworks, and accompanying guidelines aimed at protecting data privacy and regulating internet access and online safety. Regional frameworks, such as the African Union Convention on Cyber Security and Personal Data Protection ("Malabo Convention"), the Declaration of Principles on Freedom of Expression and Access to Information in Africa, and the Declaration on Internet Governance and Development, provide guiding principles that reinforce digital rights and security.[40] While these measures help shape a safer digital landscape, they largely overlook platform accountability and robust safeguards for users navigating online spaces.

22. The growing presence of AI within digital ecosystems has exposed new regulatory gaps and amplified existing concerns. Currently, no binding frameworks promote AI

[31] MMA above n 25 at 7.
[32] Id.
[33] Africa Digital Rights Hub, 'Young People, Privacy and Trust in Ghana' (2023) (accessible here) at 7.
[34] Id.
[35] Africa Digital Rights Hub above n 35 at 7.
[36] Africa Digital Rights Hub above n 35 at 9.
[37] Id.
[38] Africa Digital Rights Hub above n 35 at 9.
[39] Id.
[40] African Union Convention on Cyber Security and Personal Data Protection 27 June 2014 (accessible here); Declaration of Principles on Freedom of Expression and Access to Information in Africa 2019 (accessible here); African Declaration on Internet Governance and Development of Africa's Digital Economy 2018 (accessible here).

explainability, transparency, or fairness, and that hold big tech accountable at a regional level.[41]

23. Given these challenges, there is an urgent need for legislative and policy reform that integrates AI governance into existing regulatory frameworks. Beyond legislation, guidelines should encourage multi-sector collaboration, ensuring that AI oversight includes contributions not only from policymakers, but also from civil society, industry stakeholders, and experts within the legal profession.

24. Legal and policy frameworks governing platform accountability must be clear and adaptable. While existing frameworks such as the Continental Artificial Intelligence Strategy, the Digital Transformation Strategy for Africa, and the African Union Child Online Safety and Empowerment Policy[42] recognise the importance of enforcing measures that bolster cybersecurity and ensure the protection of expression and privacy rights online, they only enforce accountability on states and other regional actors and do not account for the unchecked powers of the platforms themselves. Accordingly, we consider it appropriate that the High Commissioner's report outline the necessity of platform accountability and consider best practices from international frameworks such as AccessNow's Platform Accountability Checklist, the Digital Services Act ("DSA"), and the Online Safety Act.[43] While platforms commit to policy adherence, robust enforcement mechanisms must be instituted to ensure compliance. A strong model to consider is the DSA, which links platforms' limited liability to their proactive efforts in removing illegal and harmful content.[44]

25. Online platforms should be required to implement and maintain policies governing content moderation, advertising practices, curation methods, and strategies for mitigating harmful content. These policies must adhere to regulatory standards that safeguard privacy, freedom of expression, access to information, and children's rights. The UNESCO guidelines on digital platform responsibilities offer a valuable reference for developing these standards.[45] Additionally, platforms must conduct risk assessments to identify and mitigate harms, particularly concerning targeted advertising and algorithmic decision-making. Regulatory bodies should oversee compliance, with enforceable penalties for violations.

26. It is thus recommended that the report underscores the importance of balancing human rights considerations, particularly in cases where privacy, freedom of expression, children's rights, and access to information intersect. These principles, as outlined in the Platform Accountability Checklist, include fairness and lawfulness in

[41] While guidelines such as the African Union's Continental Artificial Intelligence Strategy (accessible here) and the African Commission's report on the Draft Study on Human and Peoples' Rights and Artificial Intelligence, Robotics, and Other New and Emerging Technologies in Africa (accessible here) exist, they are not binding.
[42] African Union Continental Artificial Intelligence Strategy July 2024 (accessible here).
[43] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC ("DSA") (accessible here); UK Online Safety Act 2023 (accessible here); accessnow, 'Platform accountability: A rule-of-law checklist for policymakers' (2024) (accessible here).
[44] Article 22(2) of the DSA.
[45] UNESCO 'Safeguarding freedom of expression and access to information: guidelines for a multistakeholder approach in the context of regulating digital platforms' (27 April 2023) (accessible here)at paras 30-1.

data processing, purpose limitation, data minimisation, accuracy, retention limitation, personal rights to access and erasure, and integrity and confidentiality in data handling. These criteria support a rights-sensitive approach to AI regulation in online spaces and could be instrumental to the development of a governance model rooted in accountability, transparency, and user protection.

ADDITIONAL RESOURCES THAT OUTLINE GOOD PRACTICES

27. Building on the themes explored in these submissions and MMA's expertise, we encourage the High Commissioner to consider some of MMA's initiatives that could serve as good practices:

    27.1. Since 2026, MMA's Web Rangers initiative has empowered over 10,000 children aged 13–17 across South Africa through a comprehensive digital and media literacy programme. Developed with key partners,[46] the programme equips children with critical online safety, digital citizenship, and rights-based advocacy skills.[47] They use these skills to create innovative campaigns promoting safe internet usage and champion their rights in the digital world. These learners also address emerging challenges and explore exciting opportunities in an increasingly digital world, advancing their rights in line with their evolving capacities and agency.

    27.2. MMA has led efforts to develop ethical guidelines for the use of generative AI within the media sector. These guidelines highlight the importance of human oversight, transparency, algorithmic bias prevention, training and literacy, and enforcement to ensure the responsible and sustainable use of AI. Accordingly, it is recommended that detailed guidelines are developed for the ethical and sustainable use of AI in media and political arenas. To ensure that guidelines are enforced, MMA recommends that an Online Integrity Ombud ("OIO"), be established focusing on platform accountability and online disinformation. The OIO would have three main powers namely, 1) handling complaints; 2) ensuring accountability, and 3) promoting digital literacy and empowerment initiatives. The OIO, if structured right, has the potential to enable a healthy information ecosystem and promote accountable platform governance, in a manner that complies with international human rights standards.

    27.3. There is also a critical need for better, more accessible, and effective transparency reporting mechanisms for children. AI needs to be rights-based and privacy-focused for children by design and these must be the basic building blocks for AI systems that are targeted at or accessible by children.

[46] Web Ranger partners include the Department of Communication and Digital Technologies (DCDT), UNICEF, Walt Disney, Google, Meta, MTN and Falcorp.
[47] For more information see webrangers.co.za.

CONCLUSION

28. MMA outlines the abovementioned recommendations as essential, rights-based, and adaptive measures to strengthen privacy protections in AI-driven data collection and processing. We remain available to provide further guidance and support as needed.

28 May 2025
Media Monitoring Africa
Word count: 3499 words