CHILDREN'S DATA PRIVACY RIGHTS IN THE DIGITAL WORLD:
RIGHTS, REALITIES AND THE NEED FOR REFORM IN SOUTH AFRICA

MEDIA MONITORING AFRICA | CONCISE REPORT, NOVEMBER 2024

Written by Phakamile Madonsela & Avani Singh

[INTRODUCTION]

The digital environment has given rise to significant shifts both in the ways children exercise their rights and the incumbent measures required in order to safeguard these effectively. It is estimated that a child goes online for the first time every half second around the world, bringing to the fore a confluence of more children than ever before being able to get online, being able to spend more time there and being able to do so far sooner than previously the case.[1] While there can be no gainsaying the important and unprecedented opportunities that the digital environment presents for children to receive and impart information and ideas in previously unimaginable ways, it must also be recognised that this renders them vulnerable to new forms of harm such as online surveillance, exploitation and abuse, targeted advertising and profiling that may have long-term ramifications without them knowing.

The right to privacy is firmly entrenched as a fundamental human right that must be respected, protected and fulfilled in respect of all persons. This said, the imperative to safeguard this is all the more profound when it comes to the privacy rights of children. As explained by UNICEF, this traverses children's physical privacy, communications privacy and, importantly, decisional privacy as well:[2]

> "Children's right to privacy is multifaceted, and the physical, communications, informational and decisional aspects of children's privacy are all relevant in the digital world. Children's physical privacy is affected by technologies that track, monitor and broadcast children's live images, behaviour or locations. Children's communications privacy is threatened where their posts, chats, messages or calls are intercepted by governments or other actors, and children's informational privacy can be put at risk when children's personal data are collected, stored or processed. Children's decisional privacy may be affected by measures that restrict access to beneficial information, inhibiting children's ability to make independent decisions in line with their developing capacities." (Emphasis added.)

The report examines the ambit of the privacy rights of children in the digital environment, the protections afforded and the interplay with other competing rights and interests in line with the demand that the best interests of the child is of paramount importance in all matters concerning the child. While the focus here is on the right to privacy, this should be understood in the context of the full range of interlinked and interrelated digital rights more broadly.

---

[1] UNICEF, 'Protecting children online', undated (accessible here).
[2] UNICEF, 'Children's online privacy and freedom of expression', 2018 (accessible here).

This brings to the fore issues around meaningful access to the internet and digital technologies, media and information literacy, the importance of children through the stages of their maturity to learn, grow and play, and the vital role of the rights of freedom of expression and access to information in their development. In addition to children's evolving maturities, regard must also be had to issues of intersectionality across for instance race, gender, sexual orientation, socio-economic background and location.

This report is fundamentally informed by Media Monitoring Africa's engagement with the diverse range of children who comprise the Article 12 Working Group and the Web Rangers programme:

- The Article 12 Working Group is made up of Web Ranger ambassadors who have been trained in digital literacy and have a special interest in policy work. All of the Working Group members are children between the ages of 13 to 17 years old. The Article 12 Working Group members engage in ICT-related policy submissions and discussions that ensure that their voices are heard and opinions considered by policymakers and industry leaders as reflective of the positions and realities of young people today. The Article 12 Working Group members engage on ICT-related submissions to ensure that policies and decisions that affect children are more child-friendly, relevant and relatable to children and their daily lives.

- Web Rangers is a digital literacy programme designed to allow young people to gain critical skills and knowledge around online safety and critical media literacy, which they use to create innovative campaigns that promote safe internet usage and champion their rights in the digital world, and learn how to spot misinformation. More information about the Web Rangers programme can be found here.

We are deeply grateful to the members of the Article 12 Working Group and Web Rangers programme for their participation, engagement and keen insights, as well as to the parents, caregivers and educators who made their participation possible. We also extend our gratitude to the Web Rangers partners (UNICEF, Google, TikTok, Meta, Disney Walt and Falcorp),Reset.Tech Australia and Internet Society Foundation in supporting the research.

[PART I] INTERNATIONAL HUMAN RIGHTS FRAMEWORK

The right to privacy finds its overarching protection under international human rights law through article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights, and further in respect of children specifically through article 16 of the Convention on the Rights of the Child ("CRC") and article 10 of the African Charter on the Rights and Welfare of the Child ("ACRWC"). With regard to the last-mentioned, the ACRWC provides as follows:

> "No child shall be subject to arbitrary or unlawful interference with his privacy, family, home or correspondence, or to the attacks upon his honour or reputation, provided that parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children. The child has the right to the protection of the law against such interference or attacks."

While this provision is substantially similar to its counterparts in the other international instruments, the ACRWC is unique in the addition of the proviso that "parents or legal guardians shall have the right to exercise reasonable supervision over the conduct of their children". In the digital environment, the role to be played by parents and guardians can be a challenging one balanced between wanting to protect the child online while also not taking measures that could erode their rights to access and engage on the internet. The African Committee of Experts on the Rights and Welfare of the Child ("African Committee of Experts") has through General Comment on Responsibilities of the Child (2017) offered helpful guidance in explaining that a child's rights should never be compromised or violated by reference to respect for adults, and that the proviso should properly be interpreted and applied in line with the full ambit of children's rights contained in the treaty.

Similarly cognisant of the challenges this presents, the United Nations Committee on the Rights of the Child ("CRC Committee") in General Comment No. 25 on Children's Rights in Relation to the Digital Environment (2021) ("GC25") has noted that the threats faced by children to their privacy rights are manifold and multi-faceted arising in a range of different ways:[3]

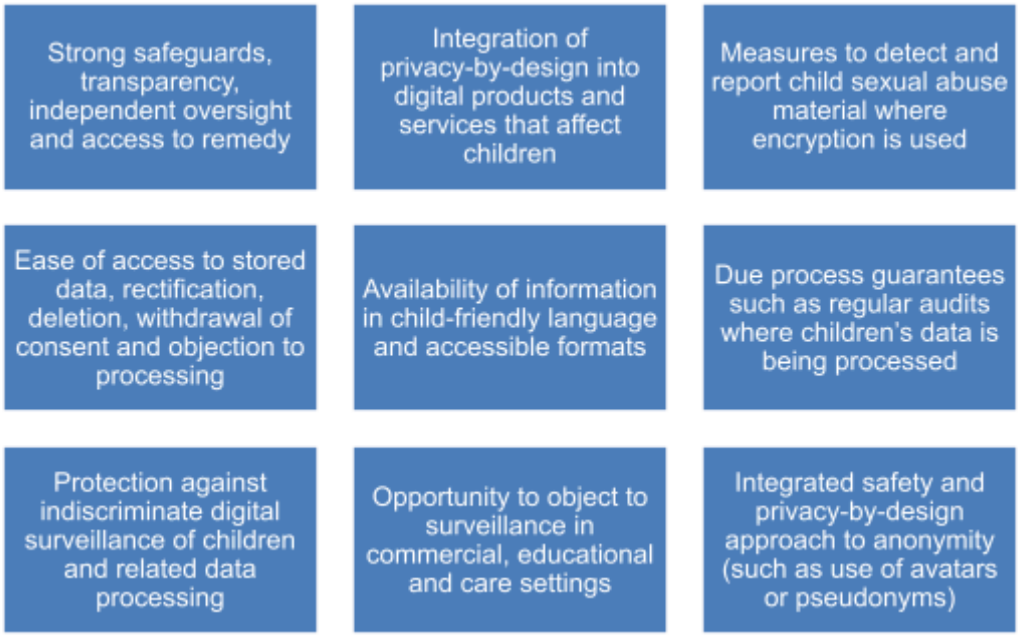
> "Children's personal data are processed to offer educational, health and other benefits to them. Threats to children's privacy may arise from data collection and processing by public institutions, businesses and other organizations, as well as from such criminal activities as identity theft. Threats may also arise from children's own activities and from the activities of family members, peers or others, for example, by parents sharing photographs online or a stranger sharing information about a child.
>
> Data may include information about, inter alia, children's identities, activities, location, communication, emotions, health and relationships. Certain combinations of personal data, including biometric data, can uniquely identify a child. Digital practices, such as automated data processing, profiling, behavioural targeting, mandatory identity verification, information filtering and mass surveillance are becoming routine. Such practices may lead to arbitrary or unlawful

[3] GC25 at paras 67-68.

interference with children's right to privacy; they may have adverse consequences on children, which can continue to affect them at later stages of their lives." (Emphasis added.)

As stated in GC25, the right to privacy is "vital to children's agency, dignity and safety and for the exercise of their rights", requiring in turn that all relevant stakeholders put in place appropriate measures to ensure this in the best interests of the child.[4] Specifically, states are required to take specific legislative, administrative and other measures to ensure that children's privacy rights are respected and protected by all organisations and in all environments that process children's information, which should be regularly reviewed and updated as needed. Furthermore, states are called on to provide advice to children, parents and caregivers on issues such as the importance of children's privacy rights and practices through which they can respect and protect children's privacy in the digital environment while still keeping them safe. For instance, it advises that the monitoring of children's digital activity by parents and caregivers should be proportionate and in accordance with the child's evolving capacities.

More generally, GC25's guidance on what would be expected of privacy and data protection frameworks to meet the necessary and appropriate standard of protection to safeguard children's privacy rights may be distilled into the following key elements:



(The Article12 Working Group also participated in the CRC Committee's consultative processes at the United Nations. The Working Group's submission can be accessed here.)

[4] GC25 at paras 67 and 70-78.

[PART II] PROTECTION OF CHILDREN'S DATA PRIVACY IN SOUTH AFRICA

The privacy rights of children are firmly entrenched in South Africa through section 14 of the Constitution of the Republic of South Africa, 1996 ("the Constitution") coupled with the guarantee of the best interests of the child being of paramount importance in section 28(2) thereof. As the Constitutional Court explained in its judgment in Centre for Child Law v Media24 Limited,[5] the analysis of the right to privacy is even more pressing when dealing with children for two key reasons: first, owing to the importance of identity and the recognition that a child's self-identity is still forming and is dependent on the approval of others; and second, due to the import of the privacy rights of young persons in fostering respect for dignity, personal integrity and autonomy, taking into account that "[t]he rights of children and their dignity and their privacy are inherently intertwined, as each child has their own 'individual dignity, special needs and interests'".

Notably, the Protection of Personal Information Act 4 of 2013 ("POPIA") is South Africa's overarching data protection law that was enacted specifically to give effect to the constitutional right to privacy in section 14 of the Constitution and contains several provisions specific to the rights of children. Although the enactment of POPIA was generally a welcomed development, the law was in fact only brought into force in 2020, some seven years after being signed into law and with a one-year grace period following thereafter, by which time POPIA was already outdated, out of sync with global best practice and with significant concerns as to it being fit for purpose. This presents a significant challenge in the meaningful protection of children's privacy rights.

The processing of the children's personal information is dealt with as a category of "special personal information" through sections 34 and 35 of POPIA in the following bifurcated way: section 34 of POPIA contains a general prohibition on processing children's personal information, stating that "[a] responsible party may … not process personal information concerning a child"; this is then attenuated by section 35 in turn, which sets out the exceptions to section 34's general prohibition. This stands to reason as a blanket ban of processing children's personal information would be a disproportionate measure and would not serve their best interests. Reading these sections together, POPIA essentially permits children's personal information to be processed only if one or more of the following instances arise:

- With prior consent of a person competent to consent on the child's behalf
- If necessary to establish, exercise or defend a legal right or defence
- If necessary to comply with an obligation of international public law
- For historical, statistical or research purposes in the public interest subject to guarantees
- Where already deliberately been made public by the child with appropriate consent

[5] [2019] ZACC 46 at paras 49-50.

The prime difficulty with these provisions is that it offers quite a blunt framework with little nuance or regard to the evolving maturities and capabilities of children to play a part in their own decisional privacy. Although the Information Regulator has published its Guidance Note on Processing of Personal Information of Children, 2020 ("POPIA Guidance Note"), this offers little assistance in interpreting and applying section 35 of POPIA in practice beyond a re-statement of the legal provisions. The Enforcement Committee of the Information Regulator, established in terms of section 93 of POPIA in August 2022, has also yet to deal with any cases specifically engaging with this issue.

For present purposes, our analysis identifies three key shortcomings in the POPIA framework insofar as it pertains to children's data privacy rights and protections. As a point of reflection, we use the European Union's General Data Protection Regulation, 2018 ("GDPR") in comparison with the approach taken in POPIA. It is important to stress here that the GDPR is by no means perfect or the gold standard per se; rather, it is simply a helpful reference point given its global prominence, relative update and ambit of its scope.

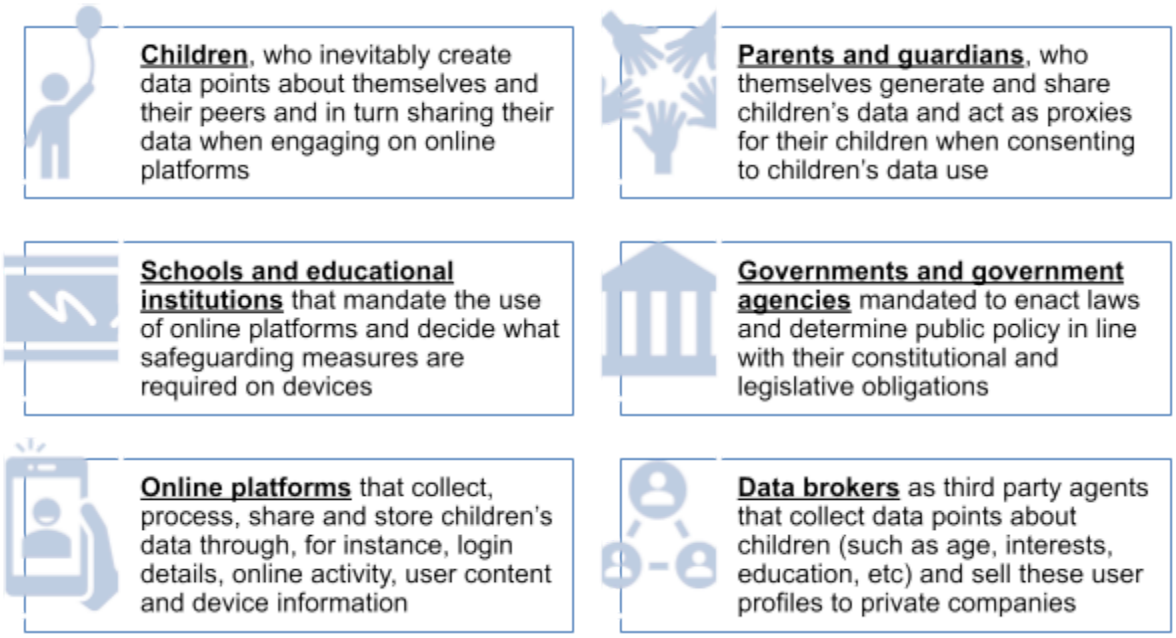
POPIA framework	Challenges	GDPR comparison
Age of consent: POPIA sets a firm age limit of 18 years for consent, meaning that any child below that age requires a legally competent person to give consent on their behalf. The term "legally competent person" is also out of sync with other child-centric laws, and in the absence of clarity has tended towards a narrow interpretation of parents and guardians alone (to the exclusion of, for instance, teachers and educators in appropriate settings).	This firm age limit is impractical in a digital age where, for example, nearly every website requires user consent to cookies notices prior to browsing. This ignores the evolving nature of children's maturities. An unduly restrictive approach may result in children not being able to access help, support or assistance in sensitive matters (such as sexual orientation or health) or where they may need protection from the parent or guardian themselves.	The GDPR provides for the age of consent at 16 years, but permits member states to provide for a lower age of 13 years and above for specific purposes. The holder of parental responsibility alone can consent on behalf of a child "taking into consideration available technology". An important addition in the recitals is that parental consent ought not to be required for counselling services being offered directly to a child. *[See articles 8 and 14 of the GDPR read with recital 38.]*

Elements of valid consent: The definition of "consent" in POPIA provides for three elements in order to be valid: (i) voluntary; (ii) specific; and (iii) informed expression of will. The responsible party bears the burden to prove the validity of the consent obtained. However, there has to date been little to no guidance provided on the content or threshold of these elements.	Consent is sometimes seen as a silver bullet to proceed with processing personal information outside of the bounds of POPIA. This has received significant attention from regulators in other jurisdictions, particularly in respect of whether it is specific and inform (as opposed to being bundled with copious clauses in the terms and services policy).	The GDPR contains two important added elements for valid consent, namely for it to be "unambiguous" and "a clear affirmative action". As the recitals advise, silence, pre-ticked boxes or inactivity should not be considered valid constitute consent. The GDPR also contains a directed provision on the conditions for a child's consent in information society services. *[See articles 4 and 8 of the GDPR read with recital 38.]*
Grounds of justification: In addition to consent, s 35 sets out a list of other possible grounds of justification that may be relied on to process a child's personal information. This includes circumstances where processing may occur unbeknown to the child or guardian, such as where it is in the public interest or involves disproportionate effort to seek consent.	Aspects of these further grounds, particularly s 35(d), are concerningly vague and can lend themselves to misuse. Ss 35(e) regarding children's information already in the public domain also brings to the fore imperative for media and information literacy skills for parents and care-givers to be able to assess the risk of what they post online and on social media.	The GDPR specifically states that children's personal information merits specific protection, taking into account that they may be less aware of the risks, consequences and safeguards. Particularly through its recitals, the GDPR offers helpful guidance in interpreting these further grounds of justification in line with the best interests of the child. *[See recital 38 to the GDPR.]*

These shortcomings in POPIA should also be seen in the light of the legislation being over ten years old, with the intervening period having seen an unprecedented rate of technological development. Much of this development has been hallmarked by the dependence on data-driven processes and outcomes, making effective data protection frameworks all the more important – both in general and in particular in order to meaningfully safeguard the privacy rights of children in accordance with states' obligation towards the best interests of the child. In recognition of this, various countries around the world have adopted or are in the process of developing child-specific data privacy frameworks directed at the implications of the digital environments on the rights and protections of children.

[PART III] GLOBAL DEVELOPMENTS IN PROTECTING CHILDREN'S PRIVACY RIGHTS

It appears to be a global reality that the regulatory ecosystem for the digital environment is often a somewhat murky spiderweb of different frameworks with overlapping and diverging elements to them. As law-makers around the globe grapple with the challenges that this presents to the meaningful protection of children's rights online – exacerbated by the regulatory lag of law-making processes being intrinsically slow and unable to keep up with the rapid pace of technological developments – different countries have taken different approaches to the development of child-specific privacy frameworks. As noted by UNICEF, the digital data ecosystem is made all the more complex as it intertwines with every part of a child's life and the involvement of a range of key players:[6]



Notably, the widespread availability of AI-driven tools such as ChapGPT has added a level of pressure on the need for effective frameworks with appropriate safeguards to protect the rights of children against risk and potentially serious harm. For purposes of this analysis, we have grouped these different approaches into three overarching categories: first, binding frameworks such as legislation; second, guidelines, codes of practice and other similar guidance frameworks; and third, sector-specific codes.

[6] UNICEF, 'The case for better governance of children's data: A manifesto', 2021 ("UNICEF Manifesto") at pp 6-7 (accessible here).

- ***Binding frameworks***

The United States' Children's Online Privacy Protection Act of 1998 ("COPPA"), which took effect in April 2000 and revised in 2013, is one example of binding legislation aimed at protecting children's privacy rights. Specifically, COPPA was a response to the rise in internet marketing targeting children in the US at the time by requiring that parental consent be obtained when collecting or using any personal information about a child under the age of 13 years. The oversight and implementation of COPPA falls within the mandate of the Federal Trade Commission, and applies to all operators of websites directed at children, with specific sections for children or whether the operator has actual knowledge of children using their website.

The main requirements imposed by COPPA for website operators are as follows: (i) a detailed privacy policy that describes the information collected from its users; (ii) verifiable parental consent to be obtained prior to collecting personal information from a child under the age of 13 years; (iii) a right for to revoke that consent and have the information deleted; (iv) disclosure to parents of any information collected on their children via the website; (v) limited collection of personal information when a child participates in online games and contests; and (vi) general requirement to protect the confidentiality, security and integrity of personal information collected online from children.[7]

There is presently a legislative package before US federal law-makers to update COPPA (referred to as 'COPPA 2.0') that would significantly expand the data privacy protections for children at a federal level if signed into law. However, the US approach remains a peculiar one given that there is no overarching data privacy framework that applies across the country, with this instead being left to individual states within the country to determine their own approach. For instance, the California Age-Appropriate Design Code Act of 2022 came into effect on 1 July 2024, with other states having introduced similar state-specific laws including Connecticut, Maryland, Minnesota, Oregon, New Jersey, New Mexico and Nevada.

- ***Guidance frameworks***

Another approach that has more commonly favoured particularly across the United Kingdom and the European Union is the development of child-specific guidance frameworks that provide more detailed content in interpreting and applying the child-specific provisions within the national data protection laws and in line with the GDPR. The Information Commissioner's Office in the United Kingdom ("ICO") was among the first to do so through its Age Appropriate Design: A code of practice for online services ("ICO Design Code"), which came into effect 2 September 2020. The ICO Design Code provides a set of 15 "flexible standards" on how to design data protection safeguards into online services to ensure they are appropriate for use by children and meet their development needs. Although not legally binding in the same way as legislation, the ICO's position is that it will bear directly in any matter involving the conduct of an online service in its scope and the sanction to be imposed.

[7] Electronic Privacy Information Centre, 'Children's privacy', undated (accessible here).

The scope of the ICO Design Code applies to "information society services likely to be accessed by children" in the United Kingdom. This includes, for instance, apps, programs, connected toys and devices, search engines, social media platforms, streaming services, online games, news and educational websites. It also includes websites that may not specifically child-focused but are "likely to be accessed" by children in the UK under the age of 18 years regardless of whether the company is UK-based or not. The ICO has taken a risk-based approach in this regard, requiring data protection impact assessments to be conducted and a focus on high levels of privacy-by-default settings that minimise the impacts of data collection and use as the default position in respect of children. The ICO Design Code has become a common model followed by data protection authorities in other countries, including in California and other US states.

In a similar vein, in December 2021 the Data Protection Commission in Ireland ("DPC") published its Fundamentals for a Child-Oriented Approach to Data Processing ("DPC Fundamentals"). According to the DPC, the principles and recommended measures are expected to be complied with by all organisations processing children's data – both on- and offline as applicable – including services that are directed at or are likely to be accessed by children. The DPC Fundamentals cover a range of data protection by design and default aspects ranging across default features and settings, transparency, tracking and profiling, user controls, parental oversight and intervention, security measures and privacy-enhancing techniques. As noted by the DPC:[8]

> "[C]omplying with an age-appropriate/child-oriented regime of data protection will involve costs and take creativity on the part of service designers, however, children are one in three users, and represent the adult market of the future. A healthy and supportive relationship with children is therefore, in the long-term, to the benefit of brands and businesses across all sectors."

In order to comply with the principles, the DPC Fundamentals essentially put forward to options: the first, described as a "floor of protection", would be for organisations to apply the requirements to the services they offer holistically so that all users – irrespective of whether they are under 18 years or not – benefit from a high, standardised level of data protection sufficient to protect the rights of any child user; or alternatively the second, to take a risk-based approach similar to the ICO Children's Code that requires the age of their users to be verified to ensure that the principles are applied where a child's personal information is being processed. It bears mention here that the DPC Fundamentals diverge from the ICO Design Code and others in an important way: instead of an age threshold, the DPC Fundamentals take the approach that children should be able to exercise their data privacy rights at any time provided they have the capacity and it is in their best interests taking into account, for instance, the age and maturity of the child, the type of request, the type of service being offered and the type of personal information at issue.

[8] DPC Fundamentals at p 8.

From a reading of the ICO Design Code and the DPC Fundamentals, it would appear that the ICO has a more rigorous expectation of compliance than the DPC, which seemingly considers the DPC Fundamentals as perhaps more advisory than binding. This attenuated approach is further illustrated through, for instance, the French data protection authority's Eight Recommendations to Enhance the Protection of Children Online, published in August 2021, which are expressly framed as being geared more towards a path to enhanced cooperation with those involved to help them become technically operational and to suggest practical advice and appropriate teaching resources. These are structured around three stakeholder groups: children, taking into account their need for autonomy and their rights while ensuring their protection online; parents and educators, to assert their role of support in the digital environment within a framework that respects the privacy and best interests of the child; and online service providers, to make them aware of their increased responsibility towards children when processing their personal information so as to offer children online services that respect their rights.

- ***Sector-specific codes of practice***

The third broad category that has been seen in this regard are approaches targeted either at a particular sector. One such example is the Council of Europe's Guidelines on Children's Data Protection in an Education Setting, published April 2021, that is specifically intended as guidance on the use of digital tools in the classroom for teaching and learning such as the use of educational technology, cloud-based services and cross-border data flows, virtual classrooms and the safeguarding measures that should be put in place. Particularly in countries without overarching data protection laws, another approach has been to build in such protections within their national ICT or broadband policies. In Rwanda, for example, the Rwanda Child Online Protection Policy that was published by the Ministry of ICT and Innovation in June 2019 identified the need to introduce data protection regulations to ensure that children's data is protected appropriated, collected only where necessary and treated with the necessary level of security and care. It specifically identified the need for any general regulations to give children's data special category status that would require higher levels of protection and introduce parental consent for the online collection and processing of younger children's data. This ultimately played a part in laying the groundwork for specific inclusion of children in the 2021 national data protection law that was enacted in the country.

The unavoidable reality at present is that there is quite simply no silver bullet to ensuring that children's privacy rights are respected, protection and fulfilled in the digital environment, with each approach having positive elements and drawbacks based on the exigencies of that country's context. This will also inevitably vary depending on external factors such as political will, effective enforcement and the sphere of influence that the state is able to exercise over the large tech companies at play. It is important here not to become overly encumbered by form over substance: the priority must be to ensure the effective and meaningful protection and realisation of children's privacy rights in the digital environment and to continue to demand that this be treated with the urgency, priority and concertedness it rightfully deserves.

[PART IV] CASE STUDY 1: ARTICLE 12 WORKING GROUP'S REVIEW OF POPIA (2022)

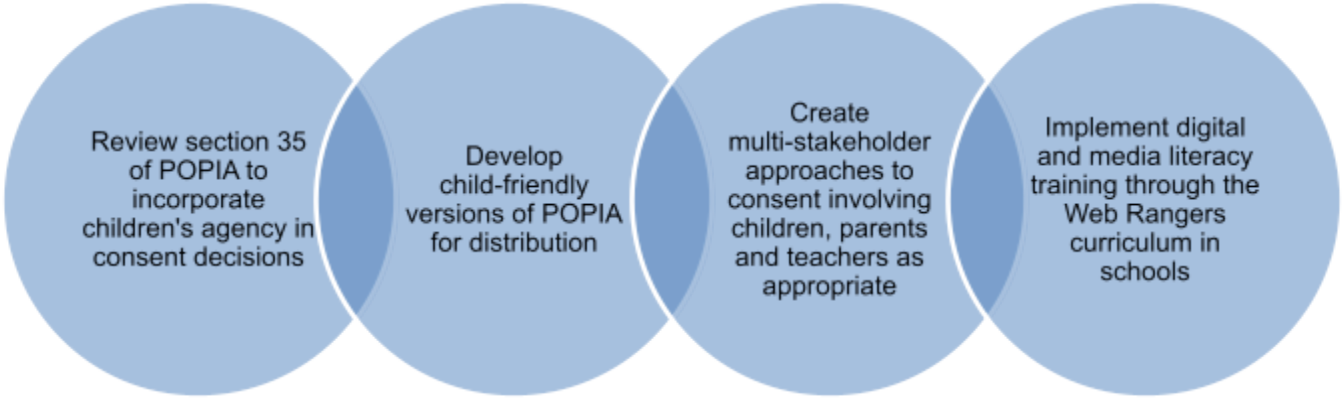
In 2022, the Article 12 Working Group composed of Web Ranger ambassadors from across undertook a review of South Africa's data privacy framework and its suitability and effectiveness in being able to protect children's privacy rights. The Working Group focused in particular on sections 34 and 35 of POPIA, which as mentioned above are the key provisions regarding the processing of children's personal information in South Africa.

While POPIA aims to protect children's data privacy rights, the Article 12 Working Group identified a significant limitation in the approach to consent and the law's failure to acknowledge children's evolving capacities and their potential to participate in decisions about their personal information. More specifically, the Working Group raised concern with the following:

- POPIA requires parental consent for processing children's personal information without children's input.
- POPIA doesn't account for varying levels of child maturity and capability (children's evolving capacities).
- No provisions exist in POPIA for shared decision-making between children, parents, and other caregivers like teachers who can also be considered guardians in a school setting.

The Working Group therefore argued for a more nuanced approach to consent, in particular that informed children should have agency in privacy decisions. In this regard, consent should be contextual, based on all relevant factors such as the child's evolving capacity, full disclosure of information usage, risk assessment and the type of personal information being shared.

In order to address this, the Working Group proposed several key reforms:



[PART V] CASE STUDY 2: CHILD-LED TECHNICAL STUDY ON SOCIAL MEDIA PLATFORM PROTECTIONS FOR CHILDREN (2024)

Building on the review of POPIA, in 2024 the Article 12 Working Group undertook a child-led technical research project that explored children's user-experiences on TikTok and Instagram within the South African context. This was done with the support and oversight of trained members of the Media Monitoring Africa team, and the full report can be accessed here.

The outcome of study resulted in four key findings that are outlined below.

1. ***The range of languages available for the terms of service (ToS) on TikTok and Instagram platforms***

In examining TikTok's language options, child researchers identified extensive coverage of European and Asian languages, with American and British English being the top two offerings. Kiswahili was the only African language option, with a generally notable absence of South African languages. This gives rise to the Working Group's main concern, that the platform does not currently support user-suggested language additions.

Instagram's language options similarly included a comprehensive coverage of European and Asian languages, with the inclusion of only one South African language – namely Afrikaans – in their language offerings.

2. ***The default privacy and safety settings on TikTok and Instagram, with a focus on how these settings affect South Africa children***

For each account set up within the context of the study, child researchers were asked to answer the question: "Does a new account for a '17 year old' default to public or private?" For a new '17 year old' account, Instagram presents both public and private account options, with no visual emphasis on the private setting. This failed to proactively guide child users towards the enhanced privacy in a simple and accessible way. TikTok defaulted new '17 year old' accounts to the public, with no prompt to choose between public or private settings.

The Article 12 Working Group further observed significant regional disparities in online safety measures, highlighting that children in South Africa do not receive the same level of digital privacy protections as their counterparts in other jurisdictions. As of September 2024, Instagram implemented enhanced privacy protections for users under 18 in select regions: default private accounts introduced in the UK, US, Canada, and Australia; and content visibility restricted to approved followers.[9] This policy has not been uniformly implemented globally, creating inconsistent protection standards for child users across different jurisdictions.

[9] BBC, 'Instagram boosts privacy and parental control on teen accounts', 14 September 2024 (accessible here).

3. ***The safety features on TikTok and Instagram, with a focus on how these features encourage protection and privacy of South Africa children***

For both applications, child researchers appreciated several key safety features such as the privacy controls that allow interaction customisation, account security through the two-step verification and regular security checks through security alerts. The family parenting page raised an important point of discussion for the child researchers, particularly regarding the statement: "Choose whether your teen can have a private or public account." Participants argued that while parental oversight is valuable, giving parents complete control over their child's privacy settings may not be ideal as some parents might lack the digital literacy skills needed to make well-informed decisions that balance their child's safety with their right privacy and other rights online.

4. ***The account deletion processes of TikTok and Instagram from a user perspective, with a focus on ease of use, clarity, and potential privacy concerns***

The Article 12 Working Group noted TikTok's straightforward approach to account deletion. The process combines accessibility with appropriate security measures, making it navigable for child users. They also appreciated TikTok's transparency efforts in the deletion process that provided them with an option to download their personal data where it had provided for data retention.

For Instagram, the participants noted that locating the deletion tab was a little more complicated when compared to TikTok. It was also noted that Instagram does a good job explaining the difference between deactivation and deletion, including asking users for their reasons to be leaving the platform. However, it is also worth noting anecdotally here that when asked for their password under the second step of the deletion process, the child researchers had forgotten their password and the process for resetting password was not user-friendly. For instance, the link sent via email did not appear to work from a mobile device and the password had to be reset using a laptop. This kind of complexity and undue formality might make some users think twice about deleting their accounts altogether despite their initial reasons for wanting to do so.

Drawing on this engagement and their personal experiences, the Article 12 Working Group developed a series of recommendations for social media platforms, the government and the Information Regulator in order to more meaningfully realise children's data privacy and other associated rights in the digital environment.

[PART VI] RECOMMENDATIONS FROM THE ARTICLE12 WORKING GROUP

Recommendations for social media platforms	
Language accessibility	There is a significant need to expand language options, particularly for African users. This expansion would ensure more inclusive access and better user understanding of privacy features across diverse communities.
Enhanced privacy protection	For users under 18, particularly in South Africa, by implementing automatic privacy-protective settings during account creation. This proactive approach would significantly improve child safety on these platforms.
User-friendly safety information	The concept and explanation of privacy on both platforms need simplification. Clear, accessible explanations would empower child users to make more informed decisions about their online privacy and security settings.
Reimagining parent-child account connections	Change the parent-child account linking process, to allow for child users to also have the power to initiate account connections during setup, so platforms can better balance parental oversight with youth privacy rights. This approach would also help prevent potential misuse of parental controls while maintaining necessary safety measures.
Platform navigation and management	Several technical improvements would enhance user experience, which include most notably the following: streamlining mobile password reset and account deletion processes; maintaining consistent placement of the settings menu (the hamburger icon) across all pages on accounts; and improving accessibility to essential features like data downloads.
Government and the Information Regulator	
Need for appropriate child-friendly laws	South African children need a version of POPIA they can understand easily, with real-life examples that make sense to them.
Autonomy and agency of children	Children should have more say in decisions about their personal information when they are capable of making these choices. The Information Regulator should review POPIA's Section 35 to give children this right where appropriate.

Media and information literacy skills built into the school curriculum	Every South African child should learn digital safety skills at school. In particular, this means— ● making digital and media literacy part of every school's curriculum; ● teaching children how to use digital media safely and responsibly; ● helping children become responsible digital citizens; and ● getting government, social media companies, and civil society organisations to work together to make this happen.
Capacity-building for parents and caregivers	Children's digital safety depends on well-informed parents. The Information Regulator should team up with key government departments (Communication and Digital Technologies, Social Development and Basic Education) to help parents understand, for instance, what POPIA means for their children; their role in protecting their children's personal information; and when and how to give consent for using their children's information.

[Ends.]