



REGULATORY

Privacy. Who is looking after the children?

28 January 2025 5 min read

As we celebrate International Privacy Day on 28 January 2025, we are called to look inward and ask how the Protection of Personal Information Act, 2013 (“**POPIA**”) has impacted South African society. But more so, has POPIA introduced greater protection for our children?

The world children live in is dominated by social network services and wearables, bringing about the “*datafication*” of almost every dimension of their lives.^[1]

POPIA was enacted on 1 July 2020. It can be seen as legislation crafted to regulate the use and disclosure of personal information, among others. During 2020 and beyond, people were bombarded with policy updates but more so requests for consent to use their personal information. But when should a child be allowed to consent to using their information? More so, at what age should children be allowed to use online services? These questions are important to consider in a time when cyberbullying is rife, harassment is ever-present, and society is confronted with an uptick in child pornography.

To understand the full complexity of children’s privacy online, we need to distinguish between interpersonal privacy, meaning how my “data self” is created, accessed and multiplied via online social connections. Institutional privacy means that our public entities, such as the government, educational institutions, and health institutions, gather and handle data. Finally, commercial privacy, i.e. how personal information is harvested and used for business purposes^[2]. It cannot be denied that there is a growing concern about people’s loss of control over their personal information, the understanding of what is public or private in the digital environment, and the number of infringements of privacy resulting from criminal activities^[3].

The importance of children in technological advancement is undeniable for various reasons. Children are often the pioneers in exploring and experimenting with new digital devices, services and content. Also, children have a less critical understanding of present and future risks to their well-being posed by using the digital environment. This means that they will engage more freely within this sphere. The question would, however, be whether children’s rights are recognised or provided for within this digital world and technological advancement.

The UNICEF Report on Children's Online Privacy and Freedom of Expression^[4] distinguishes several dimensions of privacy affected by digital technologies, i.e., physical, communication, information, and decisional privacy. Per the Report, physical privacy is violated when tracking, monitoring, or live broadcasting technologies can reveal a child's image, activities or location. Threats to communication privacy relate to access to unintended recipients' posts, chats and messages. The violation of information privacy can also occur with the collection, storage and processing of children's data, primarily if it occurs without their understanding or consent. Lastly, disruptions of decisional privacy are associated with restricting access to useful information, which can limit children's independent decision-making. This paints a complex picture and a paradox conundrum interpreting the position of children and consent.

There is no doubt that the digital world is "*data-intensive, hyperconnected and commercial*"^[5] and that an increasing amount of data, including personal information, is collected about online users, including children. The types of personal information available in the digital world impact various dimensions of privacy. Individuals about themselves or others contribute personal information, almost always knowingly, during online participation. But there is also personal information "*left*", mostly unknowingly by participation online. This personal information *is captured by data tracking technologies such as cookies, web beacons or device browsers, fingerprinting, location data*, and other metadata. This leads to *inferred data* being the data derived from analysing data given and data traces, often by algorithms, referred to as profiling, possibly combined with other data sources.^[6] Indeed, not all data types are personal information relating to an identified or identifiable individual. But it does introduce the concept of invasiveness. It also raises the question of when children consider privacy online, whether children think primarily about their privacy and the data they or others share about them online. Also, how knowledgeable are they about the data traces they leave, and how can these be used to profile them?

In a digital age in which children's communication and actions are tracked and recorded, it cannot be denied that privacy protection is vital and in their best interest. The question is, how will it play out in South Africa?

As we digitise, we must remember that children should not be mere data points; they deserve privacy and autonomy, especially in an environment that is watching their every click.

[1] Livingstone, S (2028) Children: a special case for privacy? Intermedia, 46 (2) p 18

[2] Livingstone, S. Stoilova, M. and Nandagiri, R. (2019) Children's data and privacy online: Growing up in a digital age. An evidence review. London: London School of Economics and Political Science p 3.

[3] Livingstone, S. Stoilova, M. and Nandagiri, R. (2019) Children's data and privacy online: Growing up in a digital age. An evidence review. London: London School of Economics and Political Science p 6.

[4] 2018

[5] Van der Hof, S I agree, or do I? A rights-based analysis of the law on children's consent in the digital world. Wisconsin International Law Journal 34(2) 412

[6] Livingstone, S. Stoilova, M. and Nandagiri, R. (2019) Children's data and privacy online: Growing up in a digital age. An evidence review. London: London School of Economics and Political Science p 16.



Ahmore Burger-Smidt

Head of Regulatory

[View Profile](#)