

SAFETY BY DESIGN: SAFER SOCIAL MEDIA FOR CHILDREN

Category: Privacy Law and POPIA, Privacy Law, Infosec, and POPIA
written by Kelly Lekaise | October 27, 2022



Cybercrimes are an all too real threat in cyberspace. With the growing number of internet users being children, these crimes are more likely to be targeted at the most vulnerable members of society. Ensuring the safety of children on social media is therefore important.

In South Africa, the Cybercrimes Act, 19 of 2020 (“**the Act**”) regulates cybercrimes, with most of the crimes affecting minors found in Part 2 of the Act. Activities such as child pornography, exposure to harmful content, cyberbullying, and cyber extortion are prohibited in terms of the Act.

Social media is often the gateway to these crimes since minors make use of social media platforms. Self-harm, body-dysmorphia, depression, anxiety and even death are sometimes blamed on the use of social media. It is therefore crucial that the publication of media content on social media is regulated in a way that provides the maximum protection to minors.

Social media platforms, while fostering freedom of expression, ought to monitor harmful content, that would shock the ordinary reasonable user. This is even more applicable to platforms such as TikTok and Snapchat where it is a norm for children to go to for entertainment.

The truth is that social media platforms are known to perpetuate cyber bullying, self-harm, grooming, and exposure to adult content. For example, many Facebook users have been tagged in unwanted pornographic material. Facebook has recently implemented a security feature that requires the account holder to consent to being tagged in digital content. The content is at first visible to the user

before he or she can authorise the publishing of the content on his or her page. For one to use this feature, it must first be enabled by the user. In order to promote child safety online, a feature such as this, should be the default setting. Where there are features in a platform that offer more security to the online child, these features should be the default setting. This would then allow parents to monitor the type of content their child is being tagged in, thereby preventing issues of cyberbullying and exposure to harmful content.

The above challenges can be mitigated by the same social media platforms that they occur on. It is well known that social media platforms collect various kinds of data about their users. They collect so much data that algorithms are able to tell from the data collected, details such as age, personality, likes, and dislikes of the user. Bearing this in mind, that social media platforms have insights on the age of their users, surely more protection could be offered to young children online?

Drawing from the draconian measures implemented by China to regulate online posts, the Cyberspace Administration of China published draft provisions on the responsibility of social media platforms and content creators to regulate posts on their platforms.^[1] This update requires that all social media posts including images, videos, and comments, be reviewed before they are published. Thus, it is not only in a utopian world that social media platforms can take active steps to ensure that children are protected from pornographic content, cyberbullying, cyberstalking, cyber grooming, and other online crimes that are perpetuated on the internet. This indicates the availability of tools that can be used to protect children, and accordingly, laws that promote the use of such tools should be developed. The approach highlighted above is understandably a worrisome approach when taking into account censorship and freedom of expression.

Here in South Africa, the Film and Publication Amendment Act ("**the FPAA**")^[2] has taken steps to regulate some of the content that is published by content creators. Currently all digital content that is published publicly is regulated by the FPAA. This includes a prohibition on revenge pornographic material, as well as placing an obligation on social media platforms to remove harmful content that is published on their platforms. The recent amendments require review of digital content before it is published online. The ordinary member of society is not required to submit their content to the Film and Publication Board ("**FPB**") for review, however, the FPB has the power to prosecute anyone who is reported to have published harmful content. This means that content creators still have an obligation to abide by the FPAA failing which they can be prosecuted. To this end, one can look to [a feature](#) that the social media platform Twitter has wherein where a content creator regularly posts violent or sexual content, they must flag their content as sensitive, thereby hiding the content of the post unless the audience clicks an icon to view the content. Such a feature, though not utilised by some content creators on twitter who post content without restriction, is a useful way that content creation can limit harmful content from reaching young children. Additionally, the amendments to the Children's Act, 38 of 2005 specifically recognise children's right to privacy and protection of personal information, as set out in existing legislation such the Protection of Personal Information Act, 4 of 2013. This amendment demonstrates the intention of law makers to protect children especially when using the internet since social media platforms process the personal information of children.

Lastly and most importantly, children need to be cyber aware. Although parents can monitor their children's online activities, sometimes online bullying and adult content can slip through the watchful eye of the parent. Laws can be developed, and social media platforms can be more proactive to protect children, however, this all falls short if children themselves are oblivious to the dangers they face online. It is extremely crucial for children to be able to identify when a cybercrime is being committed against them. After all, they are the main users of the internet. Children need to be aware that there are laws that protect them from certain activities online, and which channels to approach when faced with these crimes. An obligation must therefore be placed on the Department of Education to develop a curriculum that includes cybercrime awareness and how these can affect

them in their day-to-day use of the internet. The government must also ensure that teachers are regularly trained and updated on cybercrimes that affect minor children and ensure the safety of children on social media.

[Contact us](#) for more good, clear, precise advice.

[1] Notice of the Cyberspace Administration of China on Public Solicitation of Comments on the Provisions on the Administration of Internet Thread Commenting Services
http://www.cac.gov.cn/2022-06/17/c_1657089000974111.htm.

[2] Act 11 of 2019.