THE POSTING OF KIDS PHOTOS AND VIDEOS ONLINE - SHARENTING

Context

Uploading photos or videos of kids online has become a common trend. Whilst many of those who do this do it out of affection for the young ones or simply to capture moments, they are unaware of the grave risks that come along. This article seeks to unearth the risks associated with this prevalent act and how to better protect kids even while posting them.

Introduction

Sharenting , from the words "sharing' and "parenting" is the growing habit of parents or guardians to share photos , videos and any other identifying material about their children on social media. Sharenting on social media platforms such as Instagram, Facebook, Tiktok and X has been on the upward trajectory in the modern digital age. For instance according to Quintly(a German based software company that has specialized in social media analytics), approximately 1074 photos are uploaded to Instagram per second, 64,440 per minute, 3,866,400 per hour and 95 Million per day. A good chunk of these are kids photos.

In most cases, the motivation behind posting kids photos and videos online are ,but not limited to:

- ✓ Keeping the loved ones updated on the child's inner life.
- ✓ Creating a digital scrapbook or timeline for a child's growth, achievements and milestones.
- ✓ Capture fleeting moments with their kids on a day-to-day basis.
- ✓ To foster a sense of community with other parents online.
- ✓ To seek validation and affirmation through likes and comments , making them feel good about their kid.
- ✓ To create an influencer culture mainly referred to as "momfluencers" by leveraging their child's images and stories to build an online presence.

The implications

To better understand the effects of posting underage children online, we will look at it from two dimension, the "grey area" and "white area".

"The White area"

These are the consequences that can arise through legal or social structures in the society and we have control over.

For instance, the Data Protection Act of 2019 require that any publication and transmission of children material requires parental consent. Violation of this can result in fines and criminal charges depending on the nature of the breach and potential harm to the child. An example is:

- *Roma School* in Uthiru which had published pictures of its pupils on its social profiles without parental consent, resulting in a fine of Ksh. 4.5 Million, on grounds that the pictures were published without parental knowledge.

"The grey area"

This refers to the consequences that may arise with which one has no control over and "nearly" out of reach by local government's laws and policies.

To better understand this, you have to acknowledge that once you make a post on any social media platform, you lose control over it there and then. Whether or not it goes viral, how it is propagated and perceived online , how it is used , who uses it and when they use it, is not in your control anymore. This precaution should guide the kind of content you upload online. Below are the associated risk that you are not much in control of:

- ***Collection of data to train AI models*** – With the rapid boom of Artificial Intelligence, there is need to create better and more advanced AI models that are capable to mimic human behavior on a massive scale. A subfield of AI known as Generative AI(Gen AI) – which focuses on generating new data or content that resembles existing data , is fed with vast amounts data inform of images, videos, audio and text , from which they learn from and acquire the capability to regurgitate similar content. For status, the raw data used to train GPT 3.5 is 45TB of text data.(1TB = 1024GB). The conventional smartphone has a storage capacity of 64GB. You would therefore need 16 smartphones to store the data used to train GPT-3.5 .

  GPT-4 : whilst OpenAI(the parent company of Chatgpt has been quite secretive about the exact size of data used to train GPT-4, researchers estimate that approximately 13 Trillion tokens(roughly equal to 10 Trillions words) which is approximate to 60TB of raw data was used to train GPT-4.

  Guess where most if not all of the data to train these models comes from ? Yes. You guessed it right. The social media platforms, where you and I post daily. The terms and conditions we hastily agree to while creating accounts on these platforms grant these cooperations the right to sell your data to companies creating AI models.

  So the pictures and videos you upload of your kid are used to train these AI models. Picture a scenario where you would prompt an AI to generate an image and it creates one that is quite similar to your kid. Sounds chilling ?

Whilst I am not against the training of AI models, data about children being used to train AI models which they have no knowledge about and would probably be against it if they had the necessary understanding is quite concerning and as such it is needful to be mindful of your kids online footprint.

- ***Identity theft*** - The audio from videos you post can be extracted by malicious personnel who ,using softwares such as *Audacity* and *Phonexia Voice Inspector* can separate you kids voice from the audio and then clone the kids voice (replicate to say words that the speaker never uttered) to for example seem to be in duress and ask you for money. This kind of extortion has been on the rise recently. An incidence of this kind happened on 4:55pm on 20th Jan 2023 in Arizona USA where a mother, whose daughter had gone training for a ski-race, received a distress call from her "daughter" where abductors demanded a ransom of Ksh. 129 Million($1 Million). It was later established by the police the voice was AI generated . In an interview by CNN she recounted how real and genuine it sounded. A link to the whole ordeal is in the sources.

  -Deepfakes , which are videos of a person doing what they actually didn't do or appear to be in a place which they aren't , have also been used to extort money from loved one. Cases of videos being sent to parents showing kids being involved in accidents and the ask for money to rush the kid to hospital are one of the tactics being used by scammers.

- ***Digitally orchestrated kidnapping*** – Uploading content showing your kids daily routine moments makes the kid a prime target for abductors. Picture this:
  - You post your son/daughter while dressed in their school uniform, record how and when you drop him/her to school and later pick the child in the evening and post it. With this information, the abductor can know the perfect time to lure and kidnap your child. In addition , posting visits to places and the activities you undertook with the kid can be used by the abductor to initiate a conversation with the child , eventually winning their trust and easing the process of abduction.

- ***Proliferation of the kids images in child pornography sites*** – Avoid sharing pictures of children in any state of undress because some individuals use web crawlers and spiders to collect pictures and videos of kids in this state and avail them to child pornography sites. In addition, uploading content of kids in this state can wreck their reputation in future.

Recommendations

Sharing can never be 100% safe. It is a matter of balancing the risks and what parents/guardians perceive as benefits. If need arise to post you son/daughter , consider doing the following :

- ❖ Pixelate the faces of the kids .Pixelated images aren't fit for training AI models and also make it difficult for malicious people to perform any exploits.
- ❖ Include background music that overshadows the voices of people in the video before uploading. NB: This doesn't mean the voices can't be extracted. Sophisticated software can still achieve this.
- ❖ While taking selfies together with the kid, have the camera orientation such that it doesn't expose his/her face .
- ❖ Hide the child's face using emojis when posting.
- ❖ Trim them out of the picture if necessary.

The government as well, through the relevant state departments needs to actively review and enforce laws and policies that protect children in the digital space.

Conclusion:

With the knowledge dissipated by this article, take the initiative to protect your kid's digital footprint.

"*Forewarned, forearmed – to be prepared is half the victory*"

~Latin Proverb~

Sources:

www.quintly.com

The Data Protection Act 2019

www.the-star.co.ke/news

Fake abduction through voice cloning.

Authored by

Daniel Chacha Mwita