TECH HIVE ADVISORY

IKIGAI

TOWARDS BUILDING A SAFER DIGITAL ENVIRONMENT FOR CHILDREN

About Tech Hive™

Tech Hive Advisory Limited ("Tech Hive") is a technology policy advisory and research firm that provides services to private and public organisations regarding the intersection between technology, business, and law. We focus on how emerging and disruptive technologies are altering and influencing the traditional ways of doing things while acting as an innovation partner to our clients.

Our experience and capability extend across Research and Policy Advisory, Privacy and Data Protection, Regulatory Intelligence, Data Ethics, Cybersecurity, Start-Up Advisory, and Digital Health. We ensure our advice serves our clients well by having an excellent understanding of their business and the markets in which they operate through accurate policy and legislative development tracking and intelligence.

Contact: contact@techhiveadvisory.org.ng

About Ikigai™

Ikigai Innovation Initiative is a non-profit organisation set up to become the one-stop centre for technology policy in Africa. We promulgate diverse research on technology policy and legal frameworks across Africa. We also engage relevant stakeholders around the intersection of law, business, and technology and advocate for better policies for the ecosystem at large. As an advocacy centre focused on emerging technologies, policy, and research, we often work and collaborate with leading research institutes, academia, organisations, civil society, and individuals on technology policy. We also publish and contribute to whitepapers, reports, policy briefs, infographics, guides and guidance, academic journals, and publications.

Our researchers work closely with governments, stakeholders, and ecosystem players, placing evidence and academic intuition at the heart of policymaking. We bring together the latest insights, evidence, and commentary from our researchers with our one-stop-shop vision for policy by connecting policymakers, decision-makers, and practitioners with our industry-leading research. We also deliver evidence-based policy that meets the grand challenges facing society by advocating for social justice in the face of technology; sensitisation on technology policies that impact their rights and lives; and promoting digital rights and digital ethics.

Contact: policy@ikigaination.org

Contributors

Adedolapo Evelyn Adegoroye

Oyindamola Banjoko

Victoria Adaramola

Disclaimer - Usage of Research

The research is general and educational and is not intended to provide, and should not be relied on, as a source of legal advice. This information and material provided in the research may not be applicable in all (or any) situations. Accordingly, they should not be acted upon without specific legal advice based on particular circumstances.

The absence of any trademark or service mark from this list does not waive Tech Hive's and Ikigai Nation's intellectual property rights in that name, mark or logo.

INTRODUCTION

Across the world, children are at risk of being exposed to harm, abuse, violence, and exploitation in the ever-developing digital environment. In addition, the COVID-19 pandemic further plunged the world into forcefully relying on digital tools to carry out day-to-day tasks. Furthermore, millions of children have to rely on online tools for learning, playing, entertainment and connecting to friends, family and their environment.[1]

However, with all their perks and advantages, these digital tools could pose a considerable challenge to the well-being and safety of children, who are more often than not vulnerable. It then becomes essential to balance the scales by regulation, although no silver bullet exists. Who and what is to be regulated? How can the regulation be implemented? Do we cut children's access to digital tools? Should we place an obligation on parents to monitor the activities of their children online? What exactly should the plan be to protect children in today's digital environment? On what basis should children's personal data be processed? Even though the internet has evolved into a crucial tool for kids' growth, how can we create a safe online environment on a platform that wasn't created with them in mind?

How Big is the Problem of Online Harm for Children?

Spending more time online without having limitless access may increase the possibility that children will run across online predators and inappropriate material. A Netflix documentary on real-life accounts of individuals who had been conned out of millions of dollars by a man they had met online was released in 2022. Adults are not entirely safe from harm when they are online. However, it is even more fatal for children who are more often than not innocent and vulnerable.

Over time, there have been several stories of children being harmed online by people they met online. For example, in 2020, a 13-year-old was allegedly killed after resisting sexual advances by a man she talked to online.[2] In 2014, there were reports of a boy murdered by someone he met through an online gaming website.[3] In 2017 also, after a 14-year-old took her life, her family found disturbing posts about suicide and self-harm on her Instagram account.[4] The stories could go on and on, from sexual grooming online, digital kidnapping, child pornography, cyberbullying, phishing, and falling victim to scams. According to enough.org, as of February 2018, nearly half (47%) of all young people were victims of cyberbullying.[5] Sometimes children become targets online due to the amount of personal data they, their parents, and loved ones around them have put online. It is often common for parents to dote over children by posting pictures and stories about them online, which, when put together by an online predator, can be exploited to steal their identity or, even worse still, leveraged to buy the trust of children.

Harm and threat to children can occur through varying means, with some having more damning consequences and effects on children than others. For example, a 2018 survey of children's online behaviour found that approximately 60% of children who use social media had witnessed some form of bullying.[6] Cyberbullying describes situations where someone uses technology on online platforms to harass, threaten, embarrass, or target another person. It could range from spreading false rumours about a person or posting embarrassing photos or videos to making general remarks and statements against their life, family, gender, race, religion, or nationality.

Another type of online harm or threat that children may be exposed to is cyberstalking. Cyberstalking is the repeated use of technology, like social media, emails, and text messages to contact and harass someone, making them fear for their safety. Cyberstalking is a type of cyberbullying similar to in-person stalking in that it invades the target's privacy and can potentially be emotionally damaging.[7] Children may get targeted for cyberbullying or cyberstalking due to the mass of personal data they, their family members, and their loved ones might have put out from birth.

As the famous internet saying goes, "the internet never forgets." It is almost impossible to completely delete personal data that has been put out on online platforms because there is a tendency for people to store and keep data and for that personal data to be replicated, stolen, manipulated or even used for identity fraud. Parents loved ones, and children themselves may not be able to foresee how particular types of content or stories may come back to haunt them or their children five to ten years down the line.

Children may also fall victim to online scams by being deceived into giving out vital information about themselves or their families in exchange for playing games or using services they might be interested in. Deceptive designs are also usually employed to undercut children's access to making choices with design interfaces that offer no real choices. Through these, children may also be manipulated into clicking links masquerading as games to download malware or give access to the hijacking of devices. Children could also be victims of digital kidnapping[8] and manipulation through deceptive designs. For instance, children could be manipulated into racking up charges for paying for games.[9]

The list of risks and threats is quite endless and continues to grow with new developing technology, making the conversation about child protection online timely and essential.

Age Appropriate Design and International Standards

Globally, the best interest of a child principle is recognised as a child's rights principle to ensure that, despite the vulnerability of children, they are not oppressed, exploited or exposed to harm.[10] According to a survey by the American Community Survey (ACS) in 2019, 95 percent of children between the age thirteen(13) to eighteen(18) had home internet access. Specifically, eighty-eight (88) percent had access through a computer and six (6) percent relied on a smartphone for home internet access.[11] The challenge of safeguarding kids on a system that wasn't created with them in mind grows as more kids are accessing the internet The problem is exacerbated when children have access to apps that were not designed specifically for them, and even when they were, it is critical to verify that the apps or Application Programming Interfaces (APIs) are not exploitative of children's vulnerabilities.

According to a report, by the time a child is 13, their parents will have posted an average of 1,300 photos and videos of them on social media.[13] After which, this data mountain "explodes" as children themselves start engaging on the platforms — posting to social media 26 times per day, on average, and amassing nearly 70,000 posts by age 18. The datafication of children via profiling and tracking of their personal data via social media accounts and mobile applications (Apps) is resulting in a data-disadvantaged generation where children are exposed to a wide range of different types of harm online.

Regulations and legislations play very crucial roles in achieving online protection of children. They provide the confines for data processors and controllers within which they must act in relation to children's data. According to a research[14] On the child data protection legislations in fifty(50) countries, eighteen (18) of them did not have specific legislation to address the collection of children's data. At the same time, none prevented children from government surveillance. Furthermore, five(5) countries exempted their government from being regulated by data protection principles. Just as it is expected that the personal data of adults should not be used to profile them, a higher level of caution is expected when it comes to the data of minors. However, of all the countries analysed, only one(1) country prohibited the profiling of children, while nineteen(19) have restrictions in that regard[15].

Although some countries are now paying attention to it, the concept of child protection online is a topical issue that weighs heavily on children's rights, and not nearly enough regulators are paying attention globally. Some countries that have shown legal and institutional considerations for online child protection include France[16], Norway[17], Egypt[18] And the Philippines[19] Among others.

In September 2020, the Age Appropriate Design Code came into force in the United Kingdom (U.K.), giving all companies and organisations in the U.K. and non-UK residents processing children's data a one-year transition phase period to be compliant.[20] The code is made subject to sections 123 and 125(3) and (4) of the U.K.'s Data Protection Act.[21]

The code outlines fifteen(15) principles that internet services must adhere to in order to comply with and ensure that children's data is protected online. Apps, games, programmes, search engines, social media platforms, online marketplaces, content sharing services, instructional websites, linked toys and devices, and news services are the codes covered online services.

The code sets standards and explains how the General Data Protection Regulation (GDPR) applies in the context of children using digital services. Some of the standards set include the following: settings must be "high privacy" by default; only the minimum amount of personal data should be collected and retained; children's data should not usually be shared; geolocation services should be switched off by default; nudge techniques should not be used to encourage children to provide unnecessary personal data, weaken or turn off their privacy settings. The code also addresses issues of parental control and profiling.[22] The code generally creater a saner and safer environment for children online and mandates digital service providers to take a rights-respecting approach towards the privacy of children.

In the European Union(E.U.), the European Commission(E.C.) has set out an European Strategy for a Better Internet for Children to create a safe environment through age-appropriate privacy settings. The strategy mandates manufacturers, online services and network providers with the task of providing safer content for children, which extends to incorporating specific settings that enable parental controls, age rating, and content classification.[23] This strategy birthed the Better Internet for Kids that all E.U. members have incorporated. The Better Internet for Kids includes the following policy points:

- High-quality online content for children;
- National public awareness, which includes mechanisms to report content that is not safe for children;
- Creating a safer environment for children online; and
- Fighting against child sexual abuse, which includes making legislation .

The World Economic Forum has also put out a toolkit to help companies create trustworthy artificial intelligence (A.I.) for children and young people. This is part of an effort to protect children from new technologies and digital services.[25] The toolkit was developed by technologists, academics, business leaders, and youth themselves. It aspires to support responsible A.I. creation, consumption, and use so that it can be a tool that gives kids more opportunity and less risk.[26] The tool is a great resource for adults to build responsible A.I. for the next generation.

The toolkit includes guidelines for the product team and their responsibilities throughout the product's lifecycle. It also includes A.I. labelling systems to increase transparency and trust among child and youth users, their parents, and guardians, as well as a guide to help parents and guardians decide whether to buy and use A.I. products for children and youth.

The United Nations Children's Funds(UNICEF) have also released Industry Guidelines for Child Online Protection.[27] The guidelines require the digital industry to adapt the following:

- Considerations for children's rights should be incorporated into all pertinent business policies and management procedures;
- Establishing standardised procedures for handling instances of child sexual abuse;
- Creating a safer and age-appropriate online environment;
- Educating children, parents, and teachers about children's safety and their responsible use of information and communications technologies (ICT); and
- Promoting digital technology as a means for increasing civic engagement.

The guidelines also offer recommendations and checklists for how businesses in specific sectors can respect and support children's rights online. The checklists target mobile operators, internet service providers, content providers, online retailers, and app developers, user-generated content; interactive and social media service providers; national and public service broadcasting; hardware manufacturers, operating system developers; and app stores.

Also, in the United States, the Children's Online Privacy Protection Act ("COPPA") imposes specific requirements on operators of websites or online services directed at children under 13 years of age and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under the age of 13.[28]

COPPA in the United States provides that websites that target children must post privacy notices and must provide notice directly to the parents, get parental consent, allow parents to review the information collected on their children and revoke their consent to the processing of their children's data as they deem fit. The initial phase of COVID-19 caused a boom in the use of educational technology (EdTechs) platforms, as schools had to switch to virtual platforms to facilitate education. In the United States, EdTechs have become so popular that, according to Forbes, an average school district in the U.S. uses over one thousand edtech tools[29]. With the wide usage of EdTechs in the U.S., there have been attempts by EdTechs to subject children to commercial surveillance. However, in a bid to protect children from such practises, the Federal Trade Commission in the U.S. has clearly stated its intention to lend weight to bridle EdTech platforms that subject children to commercial surveillance.[30]

Under the GDPR parental consent is required to process a child's data.[31] Data controllers are also expected to present privacy notices to children in a language they can understand. In addition, children can exercise the right to erasure under GDPR, where the child is not fully aware of the risks involved in processing the information at the time consent was given. This right subsists even when the subject is no longer a child.[32]

In some countries, legal measures have been introduced to prohibit the profiling of children for advertising and sending them direct marketing communications. For example, in Sehzen province in China, a draft regulation was published in June 2021 that will classify children's data as sensitive data and prohibit profiling children's online behaviour to target them with advertisements.[33] In Kenya, direct marketing to children is prohibited.[34]

Growing Trends and Attempts at Protecting Children Online

The U.K. government is preparing to spend over half a million dollars to encourage the development of detection technologies for child sexual exploitation material (CSAM) that can be bolted on to end-to-end (E2E) encrypted messaging platforms to scan for the illegal material as part of its ongoing policy push around the internet and child safety.[35] The end goal for these technologies would be to deploy them in E2E encrypted environments to detect threats to children while not compromising users' privacy.

Furthermore, there is an update to the Online Safety Bill in Parliament.[36] to ensure that service providers use accredited technology to identify child sexual exploitation and abuse(CSEA) and quickly take it down.[37]

In 2021, Apple announced plans to deploy an update that will scan devices and detect CSAM and CSEA to prioritise children's safety online.[38] Also, Google's safety centre uses hash matching to detect CSAM and CSEA.[39] Similarly, Apple announced earlier in 2021 that it would roll out a new technology called NeuralHash to identify CSAM on a user's device without having to possess the image or know its contents.[40] Security specialists and privacy advocates, however, have expressed concern that the system might be abused by powerful actors, such as governments, to falsely accuse innocent people of crimes or trick the system into picking up other materials that authoritarian nation-states find objectionable, leading Apple to shelve its new CSAM technology.[41]

Yoti, a digital identity app raising child protection standards online, has developed a biometric age estimation technology system for children. Unlike facial-recognition systems, which establish a person's identity by comparing a real-time scan of their face with a pre-existing photo, Yoti's claims its facial analysis system does not store any biometric information, either locally or in the cloud, and immediately deletes the scan once a person's age has been verified.[42]

Although the age estimation technology could be instrumental in protecting children from accessing websites that could cause them harm, it would also increase the amount of general surveillance technology that children face on a daily basis. Furthermore, A.I. technologies are not without their limitations, with the possibility of discrimination in A.I. preferences, algorithm designs, exclusions in training data or how A.I. outputs are interpreted.[43] For context, Yoti's white paper shows that the technology is the least accurate for older females with darker skin, with an error range of up to five years. In addition, the white paper says error rates are higher in older groups with darker skin tones due to "how well-represented" they are in the training data and says environmental factors—such as weather and alcohol—have more of an impact on older people than children.[44]

The E.U. has also released a "Proposal for a Regulation of the European Parliament and of the Council, laying down rules to prevent and combat child sexual abuse"[45] to provide a uniform and harmonised framework for all countries in the E.U. The law aims to detect, report, and remove CSAM from online service platforms.

Among other things, the proposal mandates the following:

a. Communication services offering services in the E.U.'s digital market must conduct a risk assessment of the misuse of their services for the dissemination of known or new child sexual abuse material or the solicitation of children.

b. It also includes targeted obligations for service providers to detect such abuse, report it via the E.U. Centre, remove or disable access to, or block online child sexual abuse material when ordered.

c. It establishes the E.U. Centre on Child Sexual Abuse as a decentralised agency to enable the implementation of the new regulation.

With this new law, service providers like Apple may be forced to pick up their shelved CSAM detection plan amidst privacy and surveillance concerns. However, these concerns have led to the E.U. insisting on specific CSAM detection technology standards to balance the need to respect privacy rights. The standards are that the technology must be effective, reliable and avoid the collection of information, and, where the collection is necessary, it must be done in line with data minimisation principles.[46]

In France, the Commission Nationale Informatique & Libertés (CNIL), the data protection authority, made recommendations to the Parliament after carrying out a survey focused on the digital activities of minors. Following these recommendations, the Parliament has voted unanimously in favour of a law that compels manufacturers to install a free, user-friendly parental control tool on their devices to protect children from violent and pornographic content.[47]

To further protect children from any form of online exploitation and privacy infringement, the Senate in France adopted a law promulgated by the French president on the commercial use of the images of children under the age of 16 years. Under the law, child influencers will be protected under the French labour code, and there will be a need for their parents or guardians to obtain government authorisation before participating in online activities that amount to labour relations.[48]

The CNIL also made useful recommendations for the protection of children online. These recommendations include: [49]

a. Regulating the capacity of minors to act online: social networks and gaming platforms should adapt their services to suit children, minors should be informed of the use of their data, and parents should have the opportunity to request the deletion of their children's data;

b. Encouraging minors to exercise their rights online;

c. Supporting parents in digital education, which involves raising awareness among parents.

d. Seeking parental consent of one of the holders of parental authority for minors under the age of 15;

e. Promoting parental control tools that respect the privacy and interest of the child. Parental control devices must respect the proportionality (by taking into account the age and maturity level of the child and avoiding the use of intrusive devices), transparency (inform the child of parental control) and ensure data security of the minor by preventing third parties from having access to the data collected);

f. Strengthening the information and rights of minors through design. Suggested measures include the display of confidentiality policies and general conditions of use of services which meet the requirements of appropriate information for the services used by minors; designing a transparent and straightforward interface, and publishing the list of their compliance and commitments to data protection of minors in a summary and understandable format;

g. Taking steps to verify the age of children online and get parents' consent while respecting their privacy. It is suggested that the principles of data minimisation, proportionality, use of robust age control systems, implementation of a simple solution for the verification of age and parental authority, implementation of industry standards and third parties involved in age verification should be compliant with the recommendation;

h. Providing specific safeguards to protect the interests of children by setting up default privacy settings, providing for the deactivation by default of devices that profile minors, and platforms must not reuse or share the data of minors with third parties for commercial or advertising purposes.

The Existing Legal Framework for Protection of Children Online in Nigeria

In Nigeria, there have been efforts to improve child online safety codified in different laws and policies. Under the Child Rights Act 2003, the primary legislation for child protection in Nigeria, a child is defined as a person under eighteen years old.[50] Section 8 of the Act guarantees the right to a child's privacy. However, it is essential to note that only about 26 states in the federation have domesticated the Act[51] with varying amendments and variegated levels of protection that defeat some of the aims of the Act.[52]

Thus, the first problem with the concept of child protection in Nigeria is the disparity in age limits with regard to certain capacities. Article 5.5 of the Nigerian Data Protection Regulation(NDPR) Implementation Framework[53] caps the age of minors at any person below the age of thirteen. Thus, under the Implementation Framework, children who are thirteen years of age or older than thirteen years of age are not protected under the NDPR Implementation Framework. Article 5.5 of the Implementation Framework goes further to state that a data controller or data processor whose processing activities target children is to ensure that the privacy notice is made in a child-friendly form. Data controllers are responsible for making children and guardians clearly understand data processing activities before requesting consent. The conflict between a child's age under the Child Rights Act and the Data Protection Implementation Framework creates an operational problem for organisations trying to comply with the regulatory requirements.

Section 8 of the Child Rights Act also provides the right to private and family life. It states that every child is entitled to privacy, family life, home, correspondence, telephone conversation, and telegraphic communications. The provision also grants parents and

legal guardians the right to exercise reasonable supervision and control over the conduct of their children or wards. However, the Child Rights Act and the NDPR are silent on the obligation of data controllers and data processors not to exploit the personal data of children using tracking devices or coercive or deceptive consent.

The Nigerian Communications Commission in 2019 also launched an awareness programme targeted at children on safe internet practices. The awareness programme was also extended to include reviewing the National Child Online Protection document, which will consist of a Policy, Strategy, and an Action Plan[54]. The Commission also launched an information kit that advises parents and caregivers on what to do to keep children and their wards safe online These activities aim to identify cyberspace risks and sensitivities for children, raise awareness, and disseminate information and experience.
In addition, part nine of the National Cybersecurity Strategy discusses a national strategy for online child abuse and exploitation. This part discusses various strategic areas of focus, which include:

- The policy suggests integrating child online abuse and exploitation regulation into the National legislation on cybercrime, the CyberCrime (Prohibition, Prevention, etc.) Act 2015. This would aim to ensure that there is an adequate body of rules to protect children and their privacy online.

- The policy adopts a multi-stakeholder approach for all stakeholders (government, regulators, law enforcement officials, app/platform owners and website operators) to harmonise collaborative efforts to protect children online;

- The policy establishes a unit under the National Cybersecurity Coordinating Center (NCCC) to handle matters relating to Child Online Abuse and Exploitation within the scope National Cybersecurity Policy.

- The policy establishes Child Online Abuse and Exploitation Protection Strategy (COAEPS) Unit under the National Cybersecurity Coordinating Center (NCCC) that will collaborate with industry regulators and operators to implement a coherent Countermeasures Technical Mechanisms (CTM) to prevent access to websites identified as hosting contents that are offensive to children and to implement processes to enable the removal of any child sexual abuse content posted on their services.

- The unit will train and build the capacity of Nigerian Law enforcement officers to conduct investigations into internet-related crimes against children and young people and maintain a register of convicted online crime offenders. In addition, the unit will also drive public awareness campaigns on the safety and security of Nigerian children's interactions online.

- The NCCC provides a working mechanism to provide a means for reporting illegal content found in the country's cyberspace, as well as quick response procedures and timelines for every report received.

- The NCCC is also tasked with promoting software which can help screen and detect child online abuse and exploitation.

Section 23 (3) of the Cybercrimes (Prevention and Prohibition) Act[57] Also, criminalising children's online engagement for sexual activities, pornographic performances, defrauding, forcing or threatening them is liable to imprisonment of up to fifteen years and/or a fine of up to twenty-five million(N25,000,000) or both.

The Nigeria Communications Commission also published a guideline during the COVID-19 period to address the increased access of children to the internet due to the pandemic. The guidelines discuss what to do to keep children safe online, the risks children face online, child online safety talking points between parent/carer and a child and tips on how to help protect children online.[58]

Amidst the bits and pieces of legislation that seek to make reference to the protection of children online, Nigeria still does not have a comprehensive law that addresses online service providers and designs that target children or are likely to be accessed by children. As a result, Nigerian and, by extension, African regulators are way behind in creating guidelines that address the privacy risks and harm that African children are exposed explicitly to.

Recommendations for the Protection of Children Online

Regulators

- Providing a robust, effective, and enforceable legal framework for protecting children online is usually the first step to protecting children online. In addition, these frameworks would function to place an obligation on both parents and service providers to maintain specific standards and practices ideal for protecting children.

- Policymakers and regulators must go beyond the scope of putting together regulations, policies, and guidelines to implement and enforce strategic means of enforcing the provisions without affecting children's privacy. For example, mandating companies to verify the ages of children before providing them access to services is not barely enough to protect children. Regulators need to be actively involved in how these tech companies intend to bring to life the letters of the law to ensure a bigger problem is not created.

- Regulators need to adopt a multi-stakeholder approach with the government, tech companies and law enforcement to tackle child exploitation online rather than.

- Governments are urged to provide regulatory agencies more power to create standards for children's rights and ICTs, especially when penalising bad actors. For instance, Google's SafeSearch Filters function will block sites that contain explicit sexual content.

- A review of the age of consent under the NDPR implementation framework to eighteen(18) years. With the age of the minority being set at twelve(12) years and below under the NDPR implementation framework[59] it is essential to understand how ideal this reduced age gap is in the grand scheme of things. According to the National Society for the Prevention of Cruelty to Children (NSPCC Learning), children aged 9-16 are particularly vulnerable to:[60]

    - seeing sexual images online;
    - seeing online content that promotes potentially harmful behaviour, such as pro-anorexia or self-harm sites; and
    - being bullied online (Mascheroni and Cuman, 2014).

Teenagers and adolescents are the categories of children that engage in more reckless, risky, and thrill-seeking behaviours than their younger and older peers. As a result, they have the highest rates of sexually transmitted diseases and criminal behaviours of any age group and can even drive faster than adults.[61] Thus, with an internet that offers no protection to their young, vulnerable minds, they have a wider opportunity to explore without limits, leaving them open to harmful content and all forms of sexual exploitation online.

Parents

- Parents should teach their kids to control their digital footprint by sharing personal data with only those they know and trust rather than with everyone online. Encourage them to be selective and use the privacy settings on their social media sites rather than sharing their personal data with their contacts.

- Parents need to be intentional about internet education. As soon as children start accessing the internet, parents need to talk to them about what they are reading, what sites they visit, and who they might be communicating with online. In addition, children should be made to understand the internet isn't private.

- Knowing parental controls for every tool or service your child consumes or uses is vital in controlling what your child is likely to come across and be exposed to.[62]

- Parents should teach their kids to limit who they share information with online to maintain control over their digital footprint. Encourage them to be picky and use the privacy settings on all platforms and products.

Service Providers

- Create child-friendly terms and conditions and privacy policies that are easy to understand for kids, and the mechanisms of data processing must be transparent

- Only collect and process data necessary for the function of the services being requested and provided by and for the children.

- Organisations need to adopt age-appropriate designs for products and services targeted at children or likely to be used by children to mitigate online risks.

- Employ child rights by design standards such that only the best policies and technologies available are employed for children's rights and best interests protection in all jurisdictions where their products and services are available.

- App settings must be high privacy by default, and nudge techniques should not be employed to deceive children into changing those settings.

- Processing and collecting children's personal data must always be in line with "the best interests of a child " principle.

- Under Article 35 of the EU GDPR[63] Where the processing of personal data is likely to pose a significant risk to the rights and freedoms of natural persons. This analysis will determine how the proposed processing operations will affect personal data protection. Thus, because processing children's personal data generally carries a higher risk, it is essential to carry out a DPIA on all apps or platforms designed for or likely to be assessed by children.

Conclusion

Children and adults are not the same, nor are they alike. Children still have a long way to go and are still in the process of evolving. Therefore, how they connect and interact with the outside world will have a far-reaching impact on their development and future. During the development and lifecycle of products for children or that may be accessed or are likely to be accessed by children, online service providers must be mandated by law and guided by default to do and contemplate what is in the child's best interest first. The government must also monitor the situation, refine data protection legislation to accommodate the regulation of digital services, and set principles and guidelines for online service providers to genuinely protect children.

References

1 United Nations Children's Fund (UNICEF), 'Children in a Digital World' (United Nations Children's Fund (UNICEF) 2017) <https://www.unicef.org/media/48601/file> accessed 1 August 2022.

2 'Calif. Girl, 13, Was Allegedly Killed After Resisting Sexual Advances of Man She Talked to Online' (PEOPLE.com) <https://people.com/crime/california-girl-allegedly-killed-resisted-sexual-advances-man-met-online/> accessed 31 July 2022

3 Moore A, 'I Couldn't Save My Child from Being Killed by an Online Predator' The Guardian (23 January 2016)<https://www.theguardian.com/lifeandstyle/2016/jan/23/breck-bednar-murder-online-grooming-gaming-lorin-lafave> accessed 31 July 2022

4 'Molly Russell: Did Her Death Change Social Media?' BBC News <https://www.bbc.com/news/av/uk-50186418> accessed 31 July 2022

5 'Enough Is Enough: Cyberbullying' <https://enough.org/stats_cyberbullying> accessed 31 July 2022

6 'Internet Safety for Kids: How to Protect Your Child from the Top 7 Dangers They Face Online' (usa.kaspersky.com, 5 July 2022) <https://usa.kaspersky.com/resource-center/threats/top-seven-dangers-children-face-online> accessed 31 July 2022

7 'How to Protect Your Kids From Cyberstalking' (Verywell Family) <https://www.verywellfamily.com/cyberstalking-how-to-keep-your-teen-safe-5181308> accessed 31 July 2022

8 'Instagram's "Digital Kidnappers" Are Stealing Children's Photos and Making up New Lives' (Quartz, 25 October 2018) <https://qz.com/1434858/digital-kidnapping-is-a-reminder-of-the-dangers-of-social-media/> accessed 1 August 2022.

9 Byard Duncan, 'So Your Child Racked up Unwanted Credit Card Charges Playing Video Games. Now What?' (Reveal, 3 August 2019) <http://revealnews.org/article/so-your-child-racked-up-unwanted-credit-card-charges-playing-video-games-now-what/> accessed 1 August 2022.

10 Article 4 of the African Charter on Rights and Welfare of the Child on "Best Interests of the Child and Article 3 of the United Nations Convention on Rights of a Child.

11 'COE - Children's Internet Access at Home' <https://nces.ed.gov/programs/coe/indicator/cch#:~:text=In%202019%2C%20some%2095%20percent,American%20Community%20Survey%20(ACS).&text=Specifically%2C%2088%20percent%20had%20access,smartphone%20for%20home%20internet%20access> accessed 31 July 2022

12 Baron J, 'Posting About Your Kids Online Could Damage Their Futures' (Forbes) <https://www.forbes.com/sites/jessicabaron/2018/12/16/parents-who-post-about-their-kids-online-could-be-damaging-their-futures/> accessed 31 July 2022

13 'Children Are Being "Datafied" before We've Understood the Risks, Report Warns' (TechCrunch) <https://social.techcrunch.com/2018/11/09/children-are-being-datafied-before-weve-understood-the-risks-report-warns/> accessed 31 July 2022

14 Bischoff P, 'Where in the World Is Your Child's Data Safe? 50 Countries Ranked on Their Child Data Protection Legislation (Comparitech, 24 May 2022) <https://www.comparitech.com/blog/information-security/child-data-privacy-by-country/> accessed 5 August 2022

15 Ibid

16 'Les droits numériques des mineurs | CNIL' <https:/www.cnil.fr/fr/les-droits-numeriques-des-mineurs> accessed 25 July 2022

17 Better Internet for Kids: Norway profile <https://www.betterinternetforkids.eu/documents/167024/6823249/Norway+–+BIK+Policy+Map+Infosheet+–+FINAL.pdf/d69a3a5e-8b3e-66cc-d3de-a4212e3c6e9b?t=1622798026847> accessed 5 August 2022

18 Egypt Child Online Protection Initiatives <https://www.itu.int/en/cop/Documents/profiles/egypt.pdf> accesses 5 August 2022.

19 'Philippines : House Panel Approves Bill to Strengthen Child Online Protection | Digital Watch Observatory' (27 January 2022) <https://dig.watch/updates/philippines-house-panel-approves-bill-to-strengthen-child-online-protection> accessed 5 August 2022

20 "'Explanatory Memorandum to the Age Appropriate Design Code 2020 [2020]' (GOV.UK) <https://www.gov.uk/government/publications/explanatory-memorandum-to-the-age-appropriate-design-code-2020-2020/explanatory-memorandum-to-the-age-appropriate-design-code-2020-2020> accessed 31 July 2022

21 Section 123 and 125 of the Data Protection Act 2018. https://www.legislation.gov.uk/ukpga/2018/12/section/123/enacted. Accessed 26 February 2022.

22 'Age Appropriate Design: A Code of Practice for Online Services' (28 July 2022) <https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/> accessed 31 July 2022

23 'A European Strategy for a Better Internet for Kids (BIK+) | Shaping Europe's Digital Future' <https://digital-strategy.ec.europa.eu/en/policies/strategy-better-internet-kids> accessed 31 July 2022

24 'BIK Policy Map - BIK Portal - BIK Community' (BIK Portal) <https://www.betterinternetforkids.eu/policy/bikmap> accessed 5 May 2022

25 “Artificial Intelligence for Children.” World Economic Forum, https://www.weforum.org/reports/artificial-intelligence-for-children/. accessed 26 May 2022.

26 “Artificial Intelligence for Children: A Toolkit | End Violence.” End Violence Against Children, https://www.end-violence.org/knowledge/artificial-intelligence-children-toolkit. accessed 26 May 2022.

27 The United Nations Children’s Funds (UNICEF) Guidelines for Industry on Child Online Protection https://www.unicef.org/media/66616/file/Industry-Guidelines-for-Online-Child Protection.pdf accessed 30 May 2022.

28 “Children’s Online Privacy Protection Rule (‘COPPA’).” Federal Trade Commission, 25 July 2013, http://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa.

29 Craig R, ‘The Edtech Gap Between China And The U.S.’ (Forbes) <https://www.forbes.com/sites/ryancraig/2021/07/09/the-edtech-gap-between-china-and-the-us/> accessed 18 July 2022).

30 ‘FTC to Crack Down on Companies That Illegally Surveil Children Learning Online’ (Federal Trade Commission, 19 May 2022)

31 Article 8 of the GDPR

32 Article 17 of the GDPR

33 ‘Shenzhen to Outlaw Digital Profiling of Minors in Blow to Big Tech’ (South China Morning Post, 1 June 2021) <https://www.scmp.com/tech/policy/article/3135610/shenzhen-outlaw-digital-profiling-kids-stave-big-techs-privacy> accessed 1 August 2022.

34 Article 13 (2) (b) Data Protection (General) Regulation

35 "U.K. Offers Cash for CSAM Detection Tech Targeted at E2E Encryption." TechCrunch, https://social.techcrunch.com/2021/09/08/uk-offers-cash-for-csam-detection-tech-targeted-at-e2e-encryption/. accessed 23 July 2022.

36 "Online Safety Bill: Factsheet." GOV. U.K., https://www.gov.uk/government/publications/online-safety-bill-supporting-documents/online-safety-bill-factsheet. accessed 23 July 2022.

37 Online Safety Bill, As Amended (Amendment Paper) https://publications.parliament.uk/pa/bills/cbill/58-03/0121/amend/onlinesafety_rm_rep_0706.pdf accessed 17 July 2022

38 Adi Robertson, ‘Apple’s Controversial New Child Protection Features, Explained’ (The Verge, 10 August 2021) <https://www.theverge.com/2021/8/10/22613225/apple-csam-scanning-messages-child-safety-features-privacy-controversy-explained> accessed 1 August 2022.

39 Google's Efforts to Combat Online Child Sexual Abuse Material FAQs - Transparency Report Help Center. https://support.google.com/transparencyreport/answer/10330933?hl=en#zippy=%2Cwhat-is-googles-approach-to-combating-csam%2Chow-does-google-identify-csam-on-its-platform. accessed 25 July 2022.

40 'Apple Confirms It Will Begin Scanning iCloud Photos for Child Abuse Images' (TechCrunch) <https://social.techcrunch.com/2021/08/05/apple-icloud-photos-scanning/> accessed 1 August 2022

41 "Apple's CSAM Detection Tech Is Under Fire — Again." TechCrunch, https://social.techcrunch.com/2021/08/18/apples-csam-detection-tech-is-under-fire-again/. accessed 25 July 2022.

42 "Yoti Develops Age Estimation Algorithm for Under-13s." ComputerWeekly.Com, https://www.computerweekly.com/news/252509286/Yoti-develops-age-estimation-algorithm-for-under-13s. accessed 25 July 2022.

43 Borgesius, F. "Discrimination, Artificial Intelligence, and Algorithmic Decision Making. (2018) <https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73> accessed 1 August 2022.

44 Nast, C. "This A.I. Predicts How Old Children Are. Can It Keep Them Safe?" Wired U.K. www.wired.co.uk, https://www.wired.co.uk/article/age-estimation-ai-yoti. accessed 25 July 2022.

45 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Laying down Rules to Prevent and Combat Child Sexual Abuse. 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A209%3AFIN&qid=1652451192472. accessed 20 July 2022.

46 'I.T. News, Careers, Business Technology, Reviews' (Computerworld) <https://www.computerworld.com/article/3660491/europe-puts-ahttps:/www.computerworld.com/article/3660491/europe-puts-a> accessed 4 August 2022

47 'France Moves to Further Protect Children against Online Pornography' (RFI, 19 January 2022) <https://www.rfi.fr/en/france/20220119-france-moves-to-further-protect-children-against-online-pornography> accessed 17 July 2022

48 'France: Parliament Adopts Law to Protect Child "Influencers" on Social Media (Library of Congress, Washington, D.C. 20540 USA) 'France: Parliament Adopts Law to Protect Child "Influencers" on Social Media (Library of Congress, Washington, D.C. 20540 USA) 'France: Parliament Adopts Law to Protect Child "Influencers" on Social Media (Library of Congress, Washington, D.C. 20540 USA) <https://www.loc.gov/item/global-legal-monitor/2020-10-30/france-parliament-adopts-law-to-protect-child-influencers-on-social-media/> accessed 31 July 2022

49 'Les droits numériques des mineurs | CNIL' <https:/www.cnil.fr/fr/les-droits-numeriques-des-mineurs> accessed 25 July 2022

50 Section 277 of the Child Rights Act

51 Nigeria, Partners West Africa. “Child Rights Act Tracker.” Partners West Africa Nigeria, https://www.partnersnigeria.org/childs-rights-law-tracker/. accessed 23 July 2022

52 Maishanu, A. "Jigawa Assembly Passes Child Rights Bill, Expunges Age Limit for Marriage." Premium Times Nigeria, 21 December 2021, https://www.premiumtimesng.com/regional/nwest/501952-jigawa-assembly-passes-child-rights-bill-expunges-age-limit-for-marriage.html. accessed 23 July 2022

53 Article 5.5 of the Nigerian Data Protection Regulation(NDPR) Implementation Framework

54 (‘NCC Planning Sensitisation for Nigerian Child on Safe Use of Internet - Danbatta’ <https://www.ncc.gov.ng/media-centre/news-headlines/702-ncc-planning-sensitisation-for-nigerian-child-on-safe-use-of-internet-danbatta> accessed 18 July 2022

55 NCC, “KEEPING CHILDREN SAFE ONLINE: Advice to parents and caregivers” (https://www.ncc.gov.ng/documents/885-igov-keeping-children-safe-online-advice-parents/file) accessed 19 March 2022.

56 Part Nine National Cybersecurity Strategy. https://www.cert.gov.ng/ngcert/resources/NATIONAL_CYBESECURITY_STRATEGY.pdf. accessed 30 March 2022.

57 Part 3, Section 23 (3) of the Nigeria Cybercrime Prevention Act 2015. https://www.cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf. accessed 30 March 2022.

58 Keeping Children Safe Online: Advice to Parents and Caregivers. https://www.ncc.gov.ng/documents/885-igov-keeping-children-safe-online-advice-parents/file. accessed 30 March 2022.

59 Article 5.5 of the Nigerian Data Protection Regulation(NDPR) Implementation Framework

60 “Protecting Children from Online Abuse.” NSPCC Learning, https://learning.nspcc.org.uk/child-abuse-and-neglect/online-abuse/. accessed 23 July 2022.

61 Tymula, A. et al. “Adolescents’ Risk-Taking Behavior Is Driven by Tolerance to Ambiguity.” Proceedings of the National Academy of Sciences, vol. 109, no. 42, Oct. 2012, pp. 17135–40. DOI.org (Crossref), https://doi.org/10.1073/pnas.1207144109. accessed 23 July 2022

62 Parental control and settings link for Apple, Google and Chrome -
Apple: https://support.apple.com/en-us/HT201304
Google:https://support.google.com/googleplay/answer/1075738?hl=en and
https://support.google.com/families/answer/7087030?hl=en
Youtube: https://support.google.com/youtubekids/answer/6172308?hl=en

63 Article 35 of the European Union General Data Protection Regulation <https://gdpr.eu/data-protection-impact-assessment-template/> accessed 5 August 2022


TECH HIVE
ADVISORY


IKIGAI