CITIZEN DIGITAL
Foundation
Awareness. Accountability. Action.

WITH ALICE, DOWN THE RABBIT HOLE

Speakers:

Ms. Aditi Pillai (Researcher, Citizen Digital Foundation)

Ms. Dhanya Krishnakumar (Journalist, Parent)

Ms. Aparajita Bharti (Co-Founder, The Quantum Hub & YLAC)

Ms. Chitra Iyer (Co-founder and CEO, Space2Grow)

Ms. Arnika Singh (Co-founder, Social & Media Matters)

Ms. Nivedita Krishna (Founder Director, Pacta)

Moderated by Nidhi Sudhan (Co-founder, Citizen Digital Foundation)

Total attendees: 35

Webinar on online child safety in India with CSOs, parents, and policymakers.

June 14th, 2024
3:00 – 4:30 pm

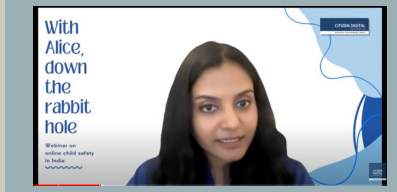
Watch on YouTube

PROBLEM AND CONTEXT

Subversive and harmful content and threats from bad actors online pose a greater threat to children and vulnerable groups in India, as evidenced in our study.

Citizen Digital Foundation conducted a virtual discussion bringing together key stakeholders of online safety in India. The webinar was titled 'With Alice, down the rabbit hole', with a focus on the powerful onslaught of recommendation algorithms that take young minds down toxic, manipulative and harmful pathways.

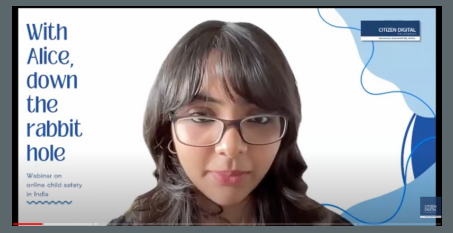
Leading online safety and children's rights organisations, and policy experts, along with parents and educators came together to discuss:
a. Building children's resilience in the online world.
b. Accountability of digital platforms.
c. Exploring policy solutions to safeguard kids online.



Context by Nidhi – Key points

- Self-determination levels in every child varies; resistance to powerful algorithmic onslaught as well.
- Acknowledge both direct & indirect harms by social media.
- Meta researches teenage brain function aimed at increasing platform engagement; findings used to manipulate children's time spent on platforms.
- Lip service by tech CEOs on child safety clashes with business model incentives.
- India yet to fully recognise platforms' power, influence and detrimental impacts on children.

CITIZEN DIGITAL Foundation
Awareness. Accountability. Action.



CDF paper presentation by Aditi - Highlights

The YouTube Rabbit Hole: Exploring Child Safety in Relation to Content in Regional Language on YouTube and YouTube Kids – CDF Study

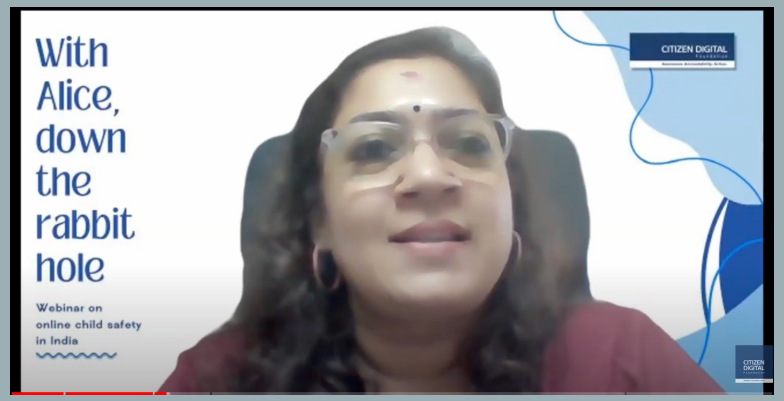
Objective: The study aimed to assess how children engage with content on YouTube and YouTube Kids in English, Hindi and Malayalam, evaluate the effectiveness of YouTube's parental controls, and understand how awareness and use of these controls can protect children.

Findings:
- Context 1 (Unrestricted YouTube Access): Harmful and inappropriate content was **easily accessible** through the recommendation system due to algorithmic incentives.
- Context 2 (Restricted Mode on YouTube): Results were largely **similar to the unrestricted context.**
- Context 3 (YouTube Kids App): Encountered content in a virtual gray area, still **posing potential risks** based on individual child's sensitivity.
- Context 4 (YouTube Kids with Restrictions): Access was limited, and all recommendations remained appropriate, providing the **safest experience.**

Summary:
- **Harmful content remains common** on YouTube and YouTube Kids, especially in Indian languages.
- YouTube's efforts to mitigate this have been **inadequate.**
- Active parental control is **essential.**
- Engagement-driven algorithms remain a **key issue.**

THE PARENT PERSPECTIVE

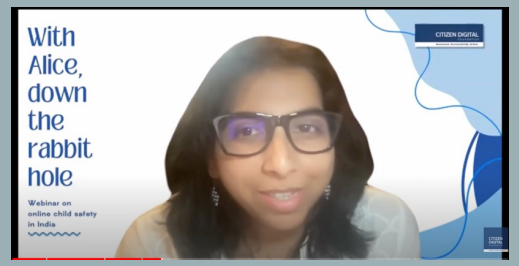
CITIZEN DIGITAL Foundation
Awareness. Accountability. Action.



Dhanya spoke about the challenges of parenting digital natives

- Raised concerns about the challenges of parenting in the digital age, focusing on balance between safety and granting access to information and freedom of expression to children online.
- Limited or no parental control over children's online activities lead to cases of children accessing inappropriate content and covering up when things go wrong.
- The dilemma of too much protection from parents leading to children facing peer pressure and cyberbullying.
- Problem of parents not discussing online safety with their children due to fear of infringing on their privacy.
- Need for more open discussions and education about online dangers among parents and children to better prepare them.
- Spoke about lack of comprehension of complexities of algorithmic targeting and limitations that even urban, well-educated parents face with dynamic online developments.

INSIGHTS FROM STUDIES



SPACE 2 GROW
Consulting for Good

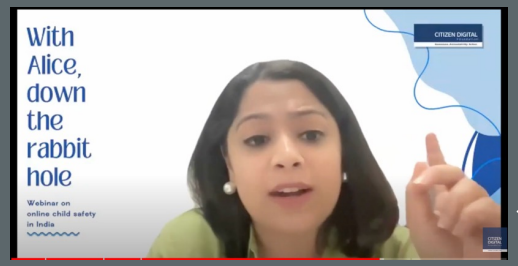
Chitra elucidates the issue through Space 2 Grow's findings

Digital Safety of Children report - Findings

- **70%** of children are online for 1 to 5 hours per day.
- **40%** of preteens use both social media and gaming platforms.
- High vulnerabilities in usage risk and behaviour; low protection indicators.
- **40%** of children have met strangers online, and **60%** of these have met offline.
- **Over 60%** of children affected by lack of social validation online.
- **Only 35%** of parents and **20%** of educators are aware of digital safety.
- **79%** of children turn to peers who are unequipped to handle digital safety issues.
- **Only 3%** of parents use mediative techniques for a safe online experience.
- **16%** of teachers reported online abuse to law enforcement.

Chitra highlights:

- High vulnerability with limited protection among children.
- Children feel they cannot live without mobile phones, indicating a dependency issue.
- The importance of parental and educational awareness is critical to addressing this issue.



CITIZEN DIGITAL
Foundation
Awareness. Accountability. Action.

TQH

Aparajita elaborates on the issue through The Quantum Hub's findings

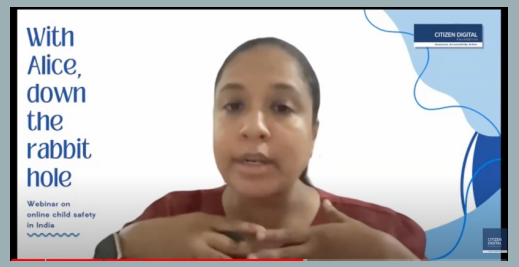
Digital Futures and DPDPA report - Findings

- **82%** of children report parents seek their help to navigate online platforms.
- High shared device usage is common; **80%** of children use shared devices.
- There's a problem with putting the **onus solely on parents** in India.
- Most parents lack the knowledge, resources, or personal devices to ensure child safety online.
- **Shared device usage** can expose children to inappropriate content inadvertently watched by parents.

Aparajita highlights:

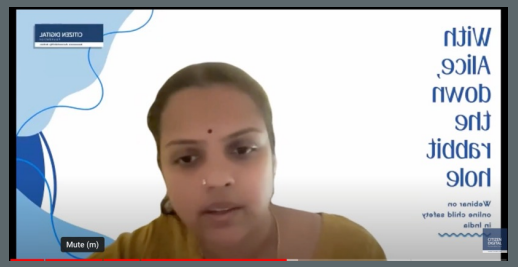
- The Indian ecosystem needs to be evaluated differently from the West.
- Putting the onus solely on parents in India won't work - most parents lack the knowledge, resources, to ensure child safety online.
- Indian schools generally prohibit carrying phones, unlike Western counterparts.
- Identifying harms in the Indian context and resolving platform design issues is crucial.
- It is important to balance access to the Internet, which provides economic opportunities, with ensuring online safety for children.

CONTEXTUALISING FOR INDIA



Arnika shares insights from Social & Media Matters' work on-ground

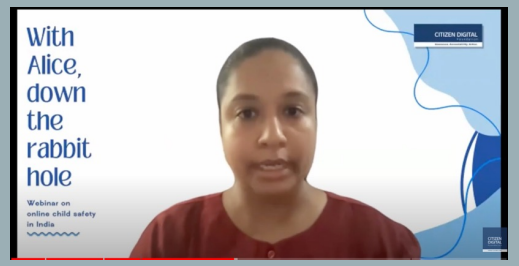
- Growing concerns regarding social media's impact on young minds, particularly related to self-harm, violence, and extremist content.
- Lack of platform accountability, effective content moderation in the absence of public pressure.
- "India changes every 2 kilometres." One-size-fits-all policies are ineffective in India's diverse socio-cultural landscape.
- Influencers in tier 2 and tier 3 cities often promote harmful content, sometimes driven by political agendas, and evade platform moderation due to algorithmic recommendations and appeals.
- Role of addictive designs in social media and its negative impact on children's mental health, citing reports indicating high levels of stress among teenagers.
- Peer pressure and the need to remain 'cool' drive teenagers to engage with potentially harmful content.
- Need to address not just individual influencers but also problematic groups and challenges such as the Blue Whale and Momo challenges.



Nivedita spoke about gaps in research and funding from Pacta's view of the ecosystem

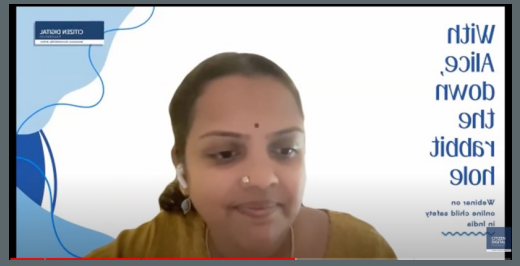
- Significant lack of funding for research in these domains in India. Such research is resource-intensive and requires substantial financial support.
- Need to document digital footprints promptly as they can disappear quickly in the digital realm, making policy approaches redundant in the absence of evidence – Shared an example about research on data monopolistic practices by food delivery platforms. The study's hypothesis changed due to market and legislative pressures during research.
- Importance of creating evidence that is demographically relevant to India.
- Currently, there's no strong market imperative for certain types of social media-related research, unlike during the pandemic when EdTech needed validation for learning outcomes.
- Comprehensive research requires diverse expertise from behavioural specialists, social scientists, data scientists, lawyers, tech policy experts, etc.
- Acknowledged excellent work done by other orgs in the space and pointed to the need for more research to be funded by Indian universities.

PLATFORM ACCOUNTABILITY & BENCHMARKING EXISTING POLICIES



Arnika talks about platforms accountability status quo

- Current content moderation approaches by platforms are failing in India.
- Proliferation of harmful and problematic content, especially inappropriate content affecting children and other vulnerable groups, supersedes any moderation attempt.
- Speeding up the redressal process for user-reported issues to build trust.
- Continue advocating for tech platforms to prioritise user safety over profit maximisation.
- Need for context-specific content moderation due to India's diverse cultural landscape.
- Need for tech platforms to engage with on-ground organisations, panels, and parents to gain a better understanding of real-world issues.

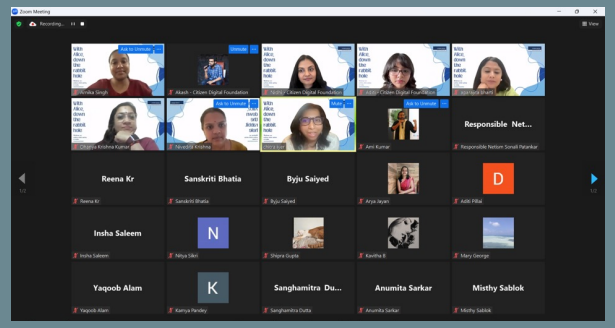


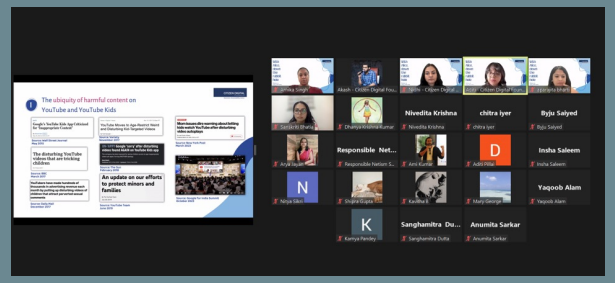
Nivedita spoke about gaps in existing policies, especially DPDPA.

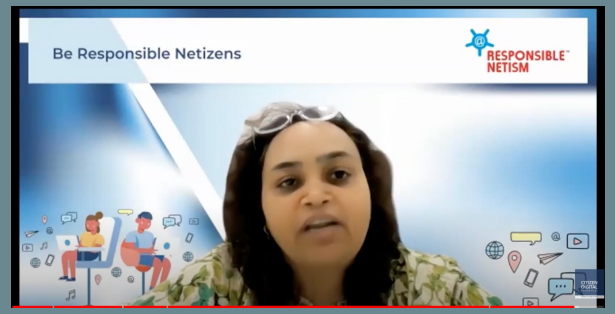
- Mention of international precedents: US more effective at state level, e.g., California's design-centric code, New York's Kid Safe Online Act. No federal law yet. Kids Online Safety Act is still waiting to be passed. UK has the Online Safety Act, which provides a safe Internet for everyone, not just children.
- Gaps in India's criminal laws regarding online offenses. India's criminal laws are broad and do not specifically define offenses like catfishing, identity theft, or grooming.
- The UK has updated its criminal laws following the Online Safety Act. India's laws lag on these updates despite having related legislations like the anti-trafficking bill. In Indian laws, offenses still fall under crimes against adults.
- DPDPA requires consent routed through parents – There are drawbacks in routing consent through parents.
- DPDPA heavily relies on citizen awareness and raising grievances.
- Lack of specification of audit and impact measurement mechanisms to verify proper implementation of DPDPA.
- Utilise international models as benchmarks for Indian policy development.
- Need for techno-legal solutions that allow parental control over algorithmic behaviours on platforms.

POSSIBLE SOLUTIONS

CITIZEN DIGITAL Foundation
Awareness. Accountability. Action.







The discussion then opened to other attendees and additional ideas and insights came in.

Experts and attendees acknowledged that online safety being a complex, multi-layered and much debated issue with several chips still in the air, no silver-bullet solution can be arrived at, especially in an emerging tech policy ecosystem in India. There were some solutions that all experts agreed on, along with unique ones. Here are the 4 key solutions discussed:

Recommendations:

1. Consortium of online safety CSOs
   a. Form a collective of all isolated efforts across India to channelise funds and resources to towards the work.
   b. Pool resources into a single bank to leverage existing work and provide substantial evidence for funders.
   c. Meet once a month as a collective to strategise actionable steps.
   d. Consortium
2. Awareness trainings – children, parents, and educators
   a. Up-to-date training of children and their first and second responders.
   b. Verified Parental Consent cannot be effective without awareness among parents.
   c. Ministry of education, social affairs should also initiate policies, not just Meity.
   d. Incorporate information literacy into school curricula.
   e. Child safety committee in schools; PTA to address issues as any other compliance.
3. Techno-legal solution:
   a. Allow parental control over algorithmic behaviours on platforms was discussed.
   b. Preset protocols in line with DPDPA that can protect children's data while ensuring their safety online and reduce cognitive burden on parents.
4. Prepare for the Digital India bill opportunity:
   a. This community can come together as a consortium to classify harms.
   b. Demand transparency of impact of algorithms, document systemic risks contextually.

REFERENCES

CITIZEN DIGITAL
Foundation
Awareness. Accountability. Action.

1. "An update on our efforts to protect minors and families". 2019. YouTube Official Blog. https://blog.youtube/news-and-events/an-update-on-our-efforts-to-protect/.
2. Bill No A08048 - Legislative Information. 2023. New York State Assembly. https://nyassembly.gov/leg/?bn=a8149&term=2023.
3. Bill No A08048 - Summary. 2023. New York State Assembly. https://nyassembly.gov/leg/?bn=a8148&term=2023.
4. "Child Online Safety: What's The Problem?". 2024. Social and Media Matters. https://www.youtube.com/watch?v=eFQarUojPdI.
5. "Children's Digital Futures and the DPDP Act 2023". 2023. YLAC Digital Champions. https://www.canva.com/design/DAF0xW2AuD0/LN3cW2pGGuNNG1N-__9qz1jg/view?utm_content=DAF0xW2AuD0&utm_campaign=designshare&utm_medium=link&utm_source=editor&continue_in_browser=true#1.
6. "Data Driven Anti-Competitive Practices of Food Service Detectors in India". 2023. PACTA. https://www.pacta.in/Food-Delivery-Platforms-Research.pdf.
7. "Digital Safety of Children: Creating Safe Online Spaces". Space 2 Grow. 2023. https://www.space2grow.in/_files/ugd/d2759d_ca7984fe036945188217ac55a516c1bc.pdf.
8. "Google for India 2023". 2023. Google India. https://www.youtube.com/watch?v=-b4lTVjOsXY.
9. "How Big Tech platforms are neglecting their non-English language users". 2023. Global Witness. https://www.globalwitness.org/en/.
10. "Impact of regulation on children's digital lives". 2024. https://eprints.lse.ac.uk/123522/1/Impact-of-regulation-on-children-DFC-Research-report.
11. "India's Dangerous Individuals & Organizations Are Being Completely Missed In Content Moderation!" 2024. Social and Media Matters. https://www.youtube.com/watch?v=_Asb9LnuGyg.

REFERENCES

CITIZEN DIGITAL Foundation
Awareness. Accountability. Action.

12. "76% Indian Parents Prefer YouTube Over OTT Platforms for Kids Animation Content: Survey". 2021. Ed Tech Review. https://www.edtechreview.in/data-statistics/76-indian-parents-prefer-youtube-over-ott-platforms-for-kids-animation-content-survey/

13. "India's Dangerous Individuals & Organizations Are Being Completely Missed In Content Moderation!". 2024. Social and Media Matters. https://www.youtube.com/watch?v=_Asb9LnuGyg.

14. "Legal Frameworks for Child Protection Online – United States, United Kingdom, India and China". 2024. Pacta. https://media.licdn.com/dms/document/media/D561FAQHL6Tt8t9FT3w/feedshare-document-pdf-analyzed/0/1718725263302?e=1720051200&v=beta&t=GZWOGhbDVI4hM7skmJ_nTSlVIsP03XCXl2STuTe61bI.

15. "Moment Mark Zuckerberg apologizes to families of children harmed online". 2024. ABC News. https://www.youtube.com/watch?v=8yIsjUXk7AQ.

16. "Mom issues dire warning about letting kids watch YouTube after disturbing video autoplays". 2023. New York Post. https://nypost.com/2023/03/23/parents-beware-if-you-let-your-children-watch-youtube-kids/.

17. Nicki Reisberg. 2024. LinkedIn. https://www.linkedin.com/posts/nickireisberg_meta-activity-7203423118588051457-B8MU?utm_source=share&utm_medium=member_desktop.

18. "Online Safety Act 2023". 2023. UK Public General Acts. https://www.legislation.gov.uk/ukpga/2023/50.

19. "The YouTube Rabbit Hole: Exploring child safety in relation to content in regional languages on YouTube and YouTube Kids". 2024. Citizen Digital Foundation. https://citizendigitalfoundation.org/publications/the-youtube-rabbit-hole-exploring-child-safety-in-relation-to-content-in-regional-languages-on-youtube-and-youtube-kids.

REFERENCES

CITIZEN DIGITAL
Foundation
Awareness. Accountability. Action.

20. “The Anxious Generation”. 2024. Jonathan Haidt. https://jonathanhaidt.com/anxious-generation/

21. The Digital Personal Data Protection Act. 2023. Ministry of Law and Justice, Government of India. https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.

22. “The disturbing YouTube videos that are tricking children”. 2017. BBC News. https://www.bbc.com/news/blogs-trending-39381889.

23. “What Is Addiction?”. Psychology Today. https://www.psychologytoday.com/us/basics/addiction.

24. “UN-'APPY Google ‘sorry’ after disturbing videos found AGAIN on YouTube Kids app”. 2018. The Sun. https://www.thesun.co.uk/tech/5514089/youtube-kids-google-sorry-inappropriate-videos/.

25. “YouTubers have made hundreds of thousands in advertising revenue each month by putting up disturbing videos of children that attract perverted sexual comments”. 2017. Mail Online. https://www.dailymail.co.uk/sciencetech/article-5170973/YouTubers-make-1-million-MONTH-disturbing-videos.html.

APPENDIX

NON-EXHAUSTIVE LIST OF RELEVANT LAWS

CITIZEN DIGITAL Foundation
Awareness. Accountability. Action.

PACTA
SOCIAL | IMPACT | LEGAL

LEGAL FRAMEWORKS FOR CHILD PROTECTION ONLINE – UNITED STATES, UNITED KINGDOM, INDIA & CHINA

Legislation	Country	Summary of Provision	Special Case Laws/Comments
Article 17 - Convention on the Rights of Child (OHCHR), 1990	International	Article 17 recognizes the important function that mass media performs and the necessity to have proper regulations to protect children from its maladies.	The Committee on the Rights of the Child published its General Comment No. 25 on Children's Rights in Relation to the Digital Environment (CRC/C/GC/25), which lays out how states parties should implement the convention in relation to the digital environment and provides guidance on relevant legislative, policy, and other measures to ensure full compliance with their obligations under the convention
Children's Online Privacy Protection Act, 1998 (COPPA)	U.S.A	COPPA applies to children under the age of 13. Defines the following terms comprehensively: Child, Operator, Disclosure, Personal information, Parent, Verifiable parental consent. It • Requires websites and online services to get verifiable parental consent before collecting, using, or disclosing personal information from children under 13. • Gives parents control over their child's information online and the ability to review or delete it. • Places obligations on website operators to ensure the security of children's data.	The COPPA is often confused with the **the Child Online Protection Act (COPA)**. COPA aimed at restricting access to harmful content for minors.Ashcroft v. American Civil Liberties Union COPA was struck down stating that less restrictive measures like filtering and blocking could be adopted.
Communications Decency Act 1996	U.S.A	Communications Decency Act 1996 prohibits anyone using interstate or communications from transmitting obscene or	Reno v. American Civil Liberties Union Landmark decision unanimously ruling that

APPENDIX

NON-EXHAUSTIVE LIST OF RELEVANT LAWS

CITIZEN DIGITAL Foundation
Awareness. Accountability. Action.

PACTA
SOCIAL | IMPACT | LEGAL

Legislation	Country	Summary of Provision	Special Case Laws/Comments
		indecent materials when they know that the recipient is under 18 years of age. **Section 230** of the Act covers protection for blocking and screening offensive material.Interactive computer services need to let customers know about the availability of parental controls to limit access to material that is harmful to minors.It also gives them the right to restrict content irrespective of whether it is constitutionally protected or not. **Section 223** provides for the protection of individuals who in good faith restrict content which is indecent, obscene and patently offensive and requires a verification process involving either a verified credit/debit account, adult.	anti-indecency provisions of the 1996 Communications Decency Act violated the First Amendment's guarantee of freedom of speech.
California Age-Appropriate Design Code Act (takes effect on July 1, 2024)	U.S.A, California	On September 15, 2022, California Age-Appropriate Design Code Act was signed. It places legal obligations on companies with respect to online products and services that are "likely to be accessed by children" under the age of 18 The Act applies to businesses that provide an online service, product or feature 'likely to be accessed by children' under the age of 18 (covered businesses). An online service, product or feature is "likely to be accessed by children" based on certain indicators, including whether: 1. It is "directed to children," as defined in COPPA.	The Act is modelled on the UK's Age-Appropriate Design Code. The California Age Appropriate Design Code is a legislative regulation that mandates businesses and online platforms to implement age-appropriate design concepts and proactively safeguard children under the age of 18 who are California residents from potential risks on the internet. This involves minimizing unnecessary data collection, prioritizing data security, and ensuring that digital interfaces are designed in the best interests of children.

APPENDIX

NON-EXHAUSTIVE LIST OF RELEVANT LAWS

CITIZEN DIGITAL Foundation
Awareness. Accountability. Action.

PACTA
SOCIAL | IMPACT | LEGAL

Legislation	Country	Summary of Provision	Special Case Laws/Comments
		2. It is determined to be routinely accessed by a significant number of children (based on competent and reliable evidence regarding audience composition) 3.It has advertisements marketed to children. 4.It is substantially similar to, or the same as, an online service, product, or feature routinely accessed by a significant number of children 5. It has design elements that are known to be of interest to children (including, but not limited to, games, cartoons, music, and celebrities who appeal to children) 6. A significant amount of the audience of the online service, product, or feature is determined, based on internal company research, to be children.	The code also requires businesses offering online services to make reasonable efforts to use visual aids, appropriate font sizes, and clear language suited to the age of the child when presenting terms of service agreements or community standards to them. This ensures that children are able to understand the terms and conditions they are agreeing to and have actual knowledge to make informed decisions about their online activities.
Stop Addictive Feeds Exploitation (SAFE) for Kids Act & the New York Child Data Protection Act	U.S.A, New York	The SAFE for Kids Act (A.8148, Rozic) will prohibit social media platforms from providing addictive feeds to children younger than 18 without parental consent. It would also require platforms to obtain parental consent in order to send notifications to children between 12:00 a.m. and 6:00 a.m. The New York Child Data Protection Act (A.8149, Rozic) will ensure that privacy is the default for minors, protecting their privacy and personal data by prohibiting online sites from	SAFE is yet to come into effect. It will go into effect 180 days after the Attorney General publishes a final set of rules and regulations that it will then enforce. The law will become effective one year after it is signed into law.

APPENDIX

NON-EXHAUSTIVE LIST OF RELEVANT LAWS

CITIZEN DIGITAL Foundation
Awareness. Accountability. Action.

PACTA
SOCIAL | IMPACT | LEGAL

Legislation	Country	Summary of Provision	Special Case Laws/Comments
		collecting, using, sharing or processing the data of individuals under the age of 18. It also prohibits operators from purchasing, selling, or allowing a third-party operator to purchase or sell personal data from users below the age of 18. "**Selling**" is defined broadly as the sharing of personal data for "monetary or other valuable consideration."	
Age-Appropriate Design Code (AADC)	U.K.	AADC, under the General Data Protection Regulation (GDPR) in force from September 2021. AADC entrusts entities handling children's data with a positive obligation to give primacy to the interests of the child. It lays down 15 standards, instead of strict dos and don'ts, directing entities to implement 'age-appropriate' design. This design should rest on principles of data minimization, purpose limitation, transparency, avoiding usage of nudge techniques, default settings that safeguard children's privacy. Virtually all entities providing online products or services - apps, programs, websites, connected toys - are covered. AADC acknowledges that the 'best interests of the child' may differ on different platforms, depending on each platform's use-case. For example, the risks on a gaming platform may be different than on a video-streaming platform. The code, therefore, encourages platforms to consider their impact on children and build in mitigation strategies.	The Information Commission Office has investigated and enforced several failures to comply with the children´s code, most recently and publically it issued a fine of £12.7 million against the social media service TikTok.

APPENDIX

NON-EXHAUSTIVE LIST OF RELEVANT LAWS

CITIZEN DIGITAL Foundation
Awareness. Accountability. Action.

PACTA
SOCIAL | IMPACT | LEGAL

Legislation	Country	Summary of Provision	Special Case Laws/Comments
Online Safety Act, 2023	U.K.	The Act will give providers new duties to implement systems and processes to reduce risks their services are used for illegal activity, and to take down illegal content when it does appear. It brings about new sets of laws to protect children as well as adults. Services must assess any risks to children from using their platforms and set appropriate age restrictions, ensuring that child users have age-appropriate experiences and are shielded from harmful content. Websites with age restrictions need to specify in their terms of service what measures they use to prevent underage access and apply these terms consistently.	This is not yet fully implemented.
Digital Services Act	European Union	Article 28 says that online platforms that can be used by minors need to make sure their services offer a high level of **privacy**, **safety** and **security** to young users Every year, Very Large Online Platforms and Very Large Online Search Engines need to **identify** and **assess** the potential online risks for children and young people using their services (Art. 34 and 35). platforms must also put **measures** in place to mitigate these risks, including (as appropriate, depending on the platforms): *Parental controls* Settings that help parents and carers, for instance, monitor or limit children's access to the internet, to protect them from online risks and inappropriate content. *Age verification* A system to check the age of users before they access the service, for instance based on physical identifiers or	The DSA became effective from Feb 24 on all platforms.

APPENDIX

NON-EXHAUSTIVE LIST OF RELEVANT LAWS

CITIZEN DIGITAL Foundation
Awareness. Accountability. Action.

PACTA
SOCIAL | IMPACT | LEGAL

Legislation	Country	Summary of Provision	Special Case Laws/Comments
		other forms of identification. *Tools* To help young people signal abuse or get support	
Advisory by the Central Government (Ministry of Education) on Online Gaming.	India	The NCPCR's Mandate is to ensure that all Laws, Policies, Programmes, and Administrative Mechanisms are in consonance with the Child Rights perspective as enshrined in the Constitution of India and as also under the UN Convention on the Rights of the Child. The Child is defined as a person in the 0 to 18 years age group. NCPCR visualizes a rights-based perspective flowing into National Policies and Programmes, along with nuanced responses at the State, District and Block levels, taking care of specificity and strengths of each region. Advisory to Parents and Teachers on Children's Safe Online Gaming with a set of dos and don'ts.	Provides cyber-crime helpline details for reporting offences.
Personal Data Protection Act, 2023 (DPDP Act)	India	The Act applies to the processing of digital personal data within India where such data is: (i) collected online, or (ii) collected offline and is digitized. It will also apply to the processing of personal data outside India if it is for offering goods or services in India. The Act requires all data fiduciaries to obtain verifiable consent from the legal guardian before processing the personal data of a child. To comply with this provision, every data fiduciary will have to verify the age of everyone signing up for its services. It will be needed to determine whether the person is a child, and thereby obtain consent from their legal guardian.	The Rules to implement the act are yet to be formulated.

APPENDIX

NON-EXHAUSTIVE LIST OF RELEVANT LAWS

CITIZEN DIGITAL Foundation
Awareness. Accountability. Action.

PACTA
SOCIAL | IMPACT | LEGAL

Legislation	Country	Summary of Provision	Special Case Laws/Comments
		The Act provides that a data fiduciary will not undertake any processing which has a detrimental effect on the well-being of the child. The Act has not defined detrimental effect. It has also not provided any guidance for determining such an effect.	
POCSO Act, 2012	India	POCSO is a key legislation governing sexual harassment of children and their protection thereof. Under the provisions of the Act, sexual assault, harassment and pornography are made punishable offences as is the abetment of any of the offences mentioned under the Act.	Though POCSO protects children from online sexual harassment, certain definitions like grooming, catfishing which are commonly adopted by perpetrators of crimes are not explicitly defined in POCSO.
Regulations on the Protection of Minors in Cyberspace read with Provisions on the Cyber Protection of Children's Personal Information ("Children Information Provisions") **issued in 2019, Minors Protection**	China	Imposes time restrictions on minors use of online games, money spent on the games. Internet product and service providers are required to establish and improve an anti-addiction system. They must not provide products and services that are addictive to minors and should change any content, functions or rules that could potentially lead to addiction. Providers are also expected to publish annual reports on their anti-addiction efforts and be open to public scrutiny. Service providers must Conduct regular impact assessments on the protection of minors online. Restriction on sharing or transmitting information harmful to minors' health such as content that promotes obscenity, pornography, violence, cults, superstition, gambling, self-harm, suicide, terrorism, separatism, extremism, etc	Regulations came into effect on January 1, 2024

APPENDIX

NON-EXHAUSTIVE LIST OF RELEVANT LAWS

CITIZEN DIGITAL Foundation
Awareness. Accountability. Action.

PACTA
SOCIAL | IMPACT | LEGAL

Legislation	Country	Summary of Provision	Special Case Laws/Comments
Law (2020 revision), and the Personal Information Protection Law ("PIPL") issued in 2021		Providers of online products and services are prohibited from using automated decision making for commercial marketing to minors. The PIPL requires options for non-personalised advertising or easy opt-out for automated decision making in personal information push and marketing. Service Providers are to take steps to reduce and mitigate cyber bullying Internet service providers offering services such as information publishing and instant messaging to minors shall legally require minors or their legal guardians to provide the minors' real identity information.	