

Navigating the Future: A Compass for Youth Policy and Practice

UNESCO Child and Family Research Centre 10th Biennial International Conference,
Galway, 9-10 June 2022

Children and Young People's Rights in a Digital World

Sonia Livingstone, London School of Economics and Political Science
@Livingstone_S www.sonialivingstone.net



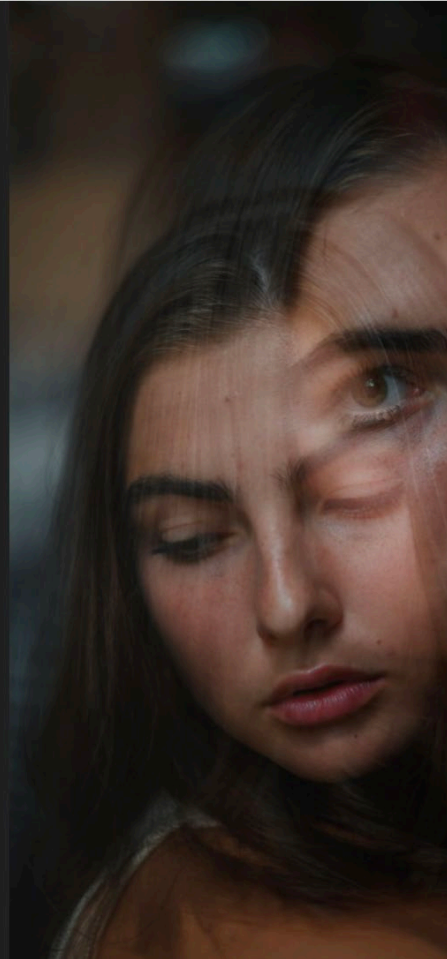
SUBSCRIBE

SIGN IN

the facebook files

Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show

Its own in-depth research shows a significant teen mental-health issue that Facebook plays down in public



[Who are you?](#)

[Products](#)

[Certifications](#)

[Resources](#)

[About Us](#)

[Contact Us](#)

How brands can connect with young audiences in the metaverse

[Download the report](#)



90% of young audiences self-identify as gamers. A robust metaverse strategy is essential to nurture engagement with the next generation.



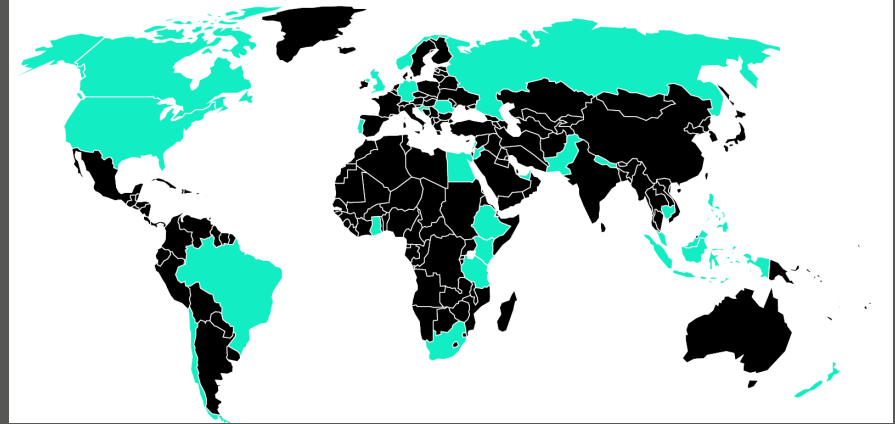
1  DEFINITION OF A CHILD	2  NO DISCRIMINATION	3  BEST INTERESTS OF THE CHILD	4  MAKING RIGHTS REAL	5  FAMILY GUIDANCE AS CHILDREN DEVELOP	6  LIFE, SURVIVAL AND DEVELOPMENT	7  NAME AND NATIONALITY	8  IDENTITY	9  KEEPING FAMILIES TOGETHER	10  CONTACT WITH PARENTS ACROSS COUNTRIES	11  PROTECTION FROM KIDNAPPING	12  RESPECT FOR CHILDREN'S VIEWS	13  SHARING THOUGHTS FREELY	14  FREEDOM OF THOUGHT AND RELIGION
15  SETTING UP OR JOINING GROUPS	16  PROTECTION OF PRIVACY	17  ACCESS TO INFORMATION	18  RESPONSIBILITY OF PARENTS	19  PROTECTION FROM VIOLENCE	20  CHILDREN WITHOUT FAMILIES	21  CHILDREN WHO ARE ADOPTED	22  REFUGEE CHILDREN	23  CHILDREN WITH DISABILITIES	24  HEALTH, WATER, FOOD, ENVIRONMENT	25  REVIEW OF A CHILD'S PLACEMENT	26  SOCIAL AND ECONOMIC HELP	27  FOOD, CLOTHING, A SAFE HOME	28  ACCESS TO EDUCATION
29  AIMS OF EDUCATION	30  MINORITY CULTURE, LANGUAGE AND RELIGION	31  REST, PLAY, CULTURE, ARTS	32  PROTECTION FROM HARMFUL WORK	33  PROTECTION FROM HARMFUL DRUGS	34  PROTECTION FROM SEXUAL ABUSE	35  PREVENTION OF SALE AND TRAFFICKING	36  PROTECTION FROM EXPLOITATION	37  CHILDREN IN DETENTION	38  PROTECTION IN WAR	39  RECOVERY AND REINTEGRATION	40  CHILDREN WHO BREAK THE LAW	41  BEST LAW FOR CHILDREN APPLIES	42  EVERYONE MUST KNOW CHILDREN'S RIGHTS

43-54

HOW THE CONVENTION WORKS

CONVENTION ON THE RIGHTS OF THE CHILD





Documents

GENERAL COMMENTS AND RECOMMENDATIONS

General comment No. 25 (2021) on children's rights in relation to the digital environment

Our Rights in the Digital World

A Report on the Children's Consultations to inform UNCRC General Comment 25

General comment No. 25 (2021) on children's rights in relation to the digital environment

I. Introduction

1. The children consulted for the present general comment reported that digital technologies were vital to their current lives and to their future. "By the means of digital technology, we can get information from all around the world", "[Digital technology] introduced us to major aspects of how I identify myself", "When you are sad, the Internet can help you [to] see something that brings you joy".

2. The digital environment is constantly evolving and expanding, encompassing information and communications technologies, including digital networks, content, services and applications, connected devices and environments, virtual and augmented reality, artificial intelligence, robotics, automated systems, algorithms and data analytics, biomimicry and implant technology.¹

3. The digital environment is becoming increasingly important across most aspects of children's lives, including during times of crisis, as societal functions, including education, government services and commerce, progressively come to rely upon digital technologies. It affords new opportunities for the realization of children's rights, but also poses the risks of their violation or abuse. During consultations, children expressed the view that the digital environment should support, promote and protect their safe and equitable engagement. "We would like the government, technology companies and teachers to help us [to] manage untrustworthy information online.", "I would like to obtain clarity about what really happens with my data ... Why collect it? How is it being collected?", "I am ... worried about my data being shared".²

4. The rights of every child must be respected, protected and fulfilled in the digital environment. Inappropriate digital technologies affect children's lives and their rights in ways that are wide-ranging and interdependent, even where children do not themselves access the Internet. Meaningful access to digital technologies can support children to realize the full range of their civil, political, cultural, economic and social rights. However, if digital inclusion is not achieved, existing inequalities are likely to increase, and new ones may arise.

5. The present general comment draws on the Committee's experience in reviewing States parties' reports, its day of general discussion on digital media and children's rights, the jurisprudence of the human rights treaty bodies, the recommendations of the Human

¹ "Our rights in a digital world", summary report on the consultation of children for the present general comment, pp. 14 and 22. Available from <https://rightsfoundation.com/uploads/Ocr%20Report%20-%20%20Digital%20World.pdf>. All references to children's views refer to that report.

² A terminology glossary is available on the Committee's webpage: https://tbinternet.ohchr.org/_layouts/15/termbodyexternal/Download.aspx?symbolno=DNT/16/CRC%20INF/25/14&lang=en.

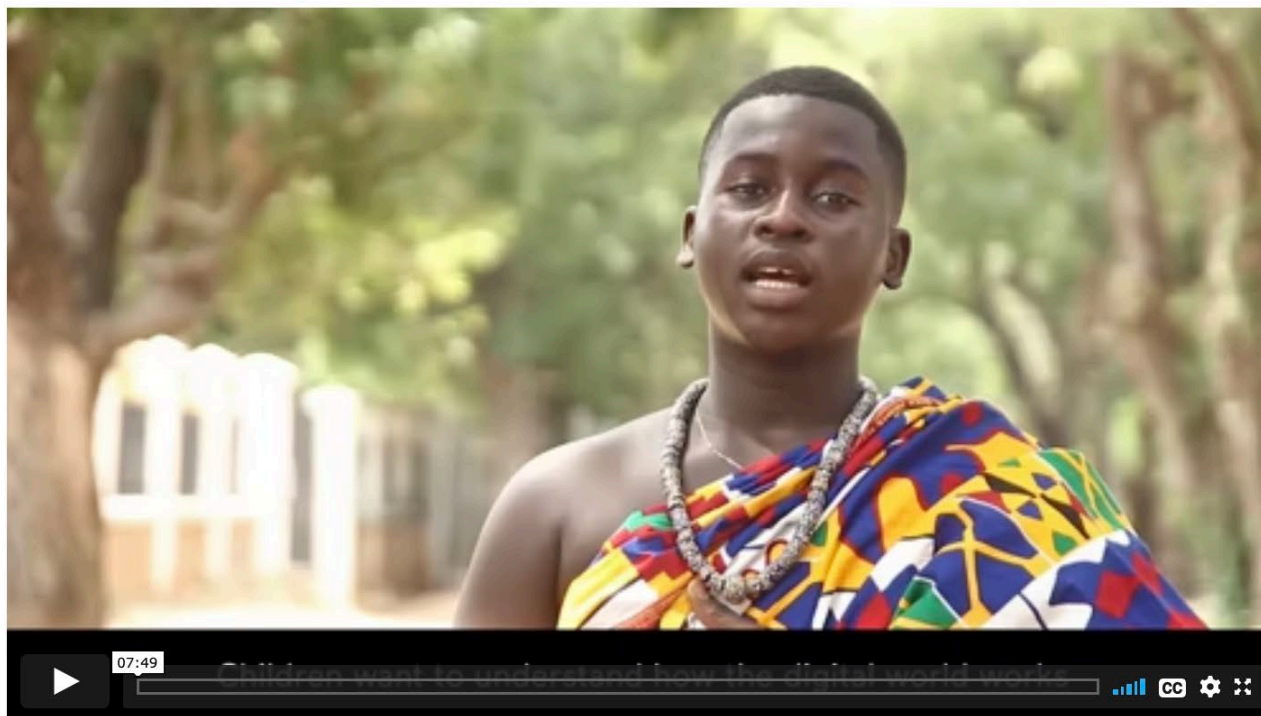
³ "Our rights in a digital world", pp. 14, 16, 22 and 25.



⁴ General comment No. 9 (2006), para. 37-38.

⁵ General comment No. 14 (2013), para. 1.

In our own words: Young people's version of general comment No. 25



Risky-by-Design

from 5Rights Foundation

Introduction	☰
The risks	
Case Study: Recommend... NEW	
Case study: Misinformation	
Case study: Friend suggestions	
Case study: Livestreaming	
Case study: In-game purchases	
About 5Rights Foundation	

INTRODUCTION

Risky by Design

Risk is a harm that has not yet happened, harm is a risk that has been realised.

Risky by design examines common design features that create risk in a series of case studies. They are not based on any one service, but each highlight how these design features pose risks to young people. Each case study takes around 5 minutes to read.

Every digital service or environment is the product of a series of design decisions that shape the experiences of young people. Low default privacy settings make a child's profile public and their identity and interests visible to strangers. Dark patterns nudge them to give up more data. False choices mean they spend money on in-game purchases in their favourite games. These design features are not neutral. They are driven primarily by commercial interests and can, individually or in combination, cause risks that can lead to harm.

Risky by design is a bold illustration of why products and services must be designed with the needs and rights of children in mind. It forms part of our broader programme of work on child-centred digital design.

37. States parties have a duty to protect children from infringements of their rights by business enterprises, including the right to be protected from all forms of violence in the digital environment. Although businesses may not be directly involved in perpetrating harmful acts, they can cause or contribute to violations of children's right to freedom from violence, including through the design and operation of digital services. States parties should put in place, monitor and enforce laws and regulations aimed at preventing violations of the right to protection from violence, as well as those aimed at investigating, adjudicating on and redressing violations as they occur in relation to the digital environment.

39. In addition to developing legislation and policies, States parties should require all businesses that affect children's rights in relation to the digital environment to implement regulatory frameworks, industry codes and terms of services that adhere to the highest standards of ethics, privacy and safety in relation to the design, engineering, development, operation, distribution and marketing of their products and services. That includes businesses that target children, have children as end users or otherwise affect children.

- “Not that there isn’t some funny stuff in there, but sometimes it’s literally all dark. I think that’s because I’ve gone through a period of, I think it was six months of pure just not getting out of this cycle. And I was just constantly watching these sad videos on TikTok. And I was just like, I’d go up to my For You page up there and it was like, sad video after sad video after sad video. I always question myself why, but then I realise that I had done this to myself because I was in such a state, such a crisis in my own head .” (18, f, mental health service user)
- “Omegle’s fine when it’s just you talking to random people just about, how’s your day, or something, or just talking about a game or something. But I’ve had people point guns at me through a camera. I’ve had things like that, because Omegle is such a weird app. So, don’t use stuff like Omegle, but still, it’s fine to talk to strangers. You can talk but just make sure it stays there, don’t give anyone personal information stuff.” (14, m, excessive gamer)
- “If you wanted to bait someone out, which is like expose them, and they’d expose naked pictures of people, and really inappropriate stuff. Someone would send it in anonymously and it would be public. It’s disgusting. Horrible. That’s children. But Snapchat never did anything about it. They didn’t ban the account.” (18, f, anxiety/suicidal)

54. States parties should protect children from harmful and untrustworthy content and ensure that relevant businesses and other providers of digital content develop and implement guidelines to enable children to safely access diverse content, recognizing children's rights to information and freedom of expression, while protecting them from such harmful material in accordance with their rights and evolving capacities. Any restrictions on the operation of any Internet-based, electronic or other information dissemination systems should be in line with article 13 of the Convention.

114. States parties should ensure that appropriate enforcement mechanisms are in place and support children, parents and caregivers in gaining access to the protections that apply. They should legislate to ensure that children are protected from harmful goods, such as weapons or drugs, or services, such as gambling. Robust age verification systems should be used to prevent children from acquiring access to products and services that are illegal for them to own or use. Such systems should be consistent with data protection and safeguarding requirements.

EU CONSENT

ELECTRONIC IDENTIFICATION AND TRUST SERVICES FOR CHILDREN IN EUROPE

Creating a safer digital world for children throughout the European Union

[CONTACT US](#)

Project objectives

The euCONSENT consortium will put into live operation extensions to the eIDAS infrastructure required to deliver its vision for pan-European, open-system, secure and certified interoperable age verification and parental consent to access Information Society Services.

Our solutions will be designed with the help of Europe's children and the guidance of the continent's leading academic experts, NGOs and other key stakeholders in child rights and protections online.

The new system will then be used during a three-month pilot by over 1,500 children, adults and parents from at least 3 EU Member States. Their user experience will be independently evaluated to provide convincing evidence for these infrastructure solutions to be adopted across the Union, with hundreds of Europe's kids already positioned as its most enthusiastic advocates to their peers, parents and policymakers.

E. Right to privacy

67. Privacy is vital to children's agency, dignity and safety and for the exercise of their rights. Children's personal data are processed to offer educational, health and other benefits to them. Threats to children's privacy may arise from data collection and processing by public institutions, companies and other organizations, and from such online practices as identifying them. There may also arise, from children's own activities and from the activities of family members, peers or others, for example, by parents sharing photographs online or a stranger sharing information about a child.

68. Data may include information about, inter alia, children's identities, activities, location, communication, emotions, health and relationships. Certain combinations of personal data, including biometric data, can uniquely identify a child. Data practices such as automated data processing, profiling, data mining, targeted advertising, identification verification and facial recognition and mass surveillance are becoming routine. Such practices may lead to arbitrary or unlawful interference with children's right to privacy; they may have adverse consequences on children, which can continue to affect them at later stages of their lives.

69. Interference with a child's privacy is only permissible if it is neither arbitrary nor unlawful. Any such interference should therefore be provided for by law, intended to serve a legitimate purpose, uphold the principle of data minimization, be proportionate and designed to observe the best interests of the child and must be in conformity with the provisions, aims and objectives of the Convention.

70. States parties should take legislative, administrative and other measures to ensure that children's privacy is respected and protected by all organizations and in all environments that process their data. Legislation should include strong safeguards, transparency, independent oversight and access to remedies. States parties should require the integration of privacy-by-design into digital products and services that affect children. They should regularly review privacy and data protection legislation and ensure that procedures and practices prevent deliberate infringements or accidental breaches of children's privacy. Where encryption is considered an appropriate means, States parties should consider appropriate measures enabling the detection and reporting of child sexual exploitation and abuse or child sexual abuse material. Such measures must be strictly limited according to the principles of legality, necessity and proportionality.

71. Where consent is sought to process a child's data, States parties should ensure that consent is informed and freely given by the child or, depending on the child's age and evolving capacity, by the parent or caregiver, and obtained prior to processing those data. Where a child's own consent is considered insufficient and parental consent is required to process a child's personal data, States parties should require that organizations processing such data verify that consent is informed, meaningful and given by the child's parent or caregiver.

72. States parties should ensure that children and their parents or caregivers can easily access stored data, rectify data that are inaccurate or outdated and delete data unlawfully or unnecessarily stored by public authorities, private individuals or other persons, subject to reasonable and lawful limitations. They should further ensure the right of children to withdraw their consent and object to personal data processing where the data controller does not demonstrate legitimate, overriding grounds for the processing. They should also provide information to children, parents and caregivers on such matters, in child-friendly language and accessible formats.

73. Children's personal data should be accessible only to the authorities, organizations and individuals designated under the law to process them in compliance with such due process guarantees as regular audits and accountability measures. Children's data gathered for defined purposes by any organization or individual should be protected and deleted once those purposes are fulfilled. Such data should not be retained unlawfully or unnecessarily or used for other purposes. Where information is provided in one setting and could legitimately benefit the child through its use in another setting, for example, in the context of schooling and tertiary education, the use of such data should be transparent, accountable and subject to the consent of the child, parent or caregiver, as appropriate.

74. Privacy and data protection legislation and measures should not arbitrarily limit children's other rights, such as their right to freedom of expression or protection. States parties should ensure that data protection legislation respects children's privacy and personal data in relation to the digital environment. Through continual technological innovation, the scope of the digital environment is expanding to include ever more services and products, such as clothes and toys. As settings where children spend time become "connected", through the use of embedded sensors connected to automated systems, States parties should ensure that the products and services that contribute to such environments are subject to robust data protection and other privacy regulations and standards. That includes public settings, such as streets, schools, libraries, sports and entertainment venues and business premises, including shops and cinemas, and the home.

75. Any digital surveillance of children, together with any associated automated processing of personal data, should respect the child's right to privacy and should not be conducted routinely, indiscriminately or without the child's knowledge or in the case of covertly obtained data. The principle of proportionality should also apply, and should take place without being in conflict with the child's right to privacy in commercial settings and educational and care settings, and consideration should always be given to the least privacy-intrusive means available to fulfil the desired purpose.

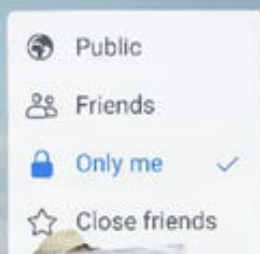
76. The digital environment presents particular problems for parents and caregivers in respecting children's right to privacy. Technologies that monitor online activities for safety purposes, such as tracking devices and services, if not implemented properly, may prevent a child from accessing a variety of services and information, which could affect children, parents and caregivers and the fulfilment of the importance of the child's right to privacy and on how their own practices may threaten that right. They should also be advised about the practices through which they can respect and protect children's privacy in relation to the digital environment, while keeping them safe. Parents' and caregivers' monitoring of a child's digital activity should be proportionate and in accordance with the child's evolving capacities.

77. Many children use online avatars or pseudonyms that protect their identity, and such practices can be important in protecting children's privacy. States parties should require an approach integrating safety-by-design and privacy-by-design to maximize child online safety while ensuring that anonymous practices are not routinely used to hide harmful or illegal behaviour, such as cyberstalking, hate speech or sexual exploitation and abuse. Protecting a child's privacy in the digital environment may be vital in circumstances where parents or caregivers themselves pose a threat to the child's safety or where they are in conflict over the child's care. Such cases may require further intervention, as well as family counselling or other services, to safeguard the child's right to privacy.

78. Access to private or sensitive services, such as online health services, should be subject to a requirement for consent to use to obtain essential services in order to access such services. Such services should be held to high standards of privacy and child protection.

We all have our own privacy settings

So when it comes to your privacy on Facebook, we think you should have the same control. From the ads you see to your personal details, choose the settings that are right for you at facebook.com/privacy



facebook

Share with my school, GP, future employer

Personal information

- Home address
- Telephone number
- Email address

Identity information

- Date of birth
- Full name
- Gender

Sensitive information

- Religious or spiritual activities
- Body weight
- Your mental health

Share with my online contacts

Identity information

- Date of birth
- Full name
- Gender

Preferences

- Films & music you like
- Food you eat
- Things you like to buy

Share with companies (advertising, profiling)

Personal information

- Home address
- Telephone number
- Email address

Web browsing

- Sites I visited
- Frequency of visits
- Adverts clicked

Preferences

- Films & music you like
- Food you eat
- Things you like to buy

Identity information

- Full name
- Gender

Keep to myself and not share online

Web browsing

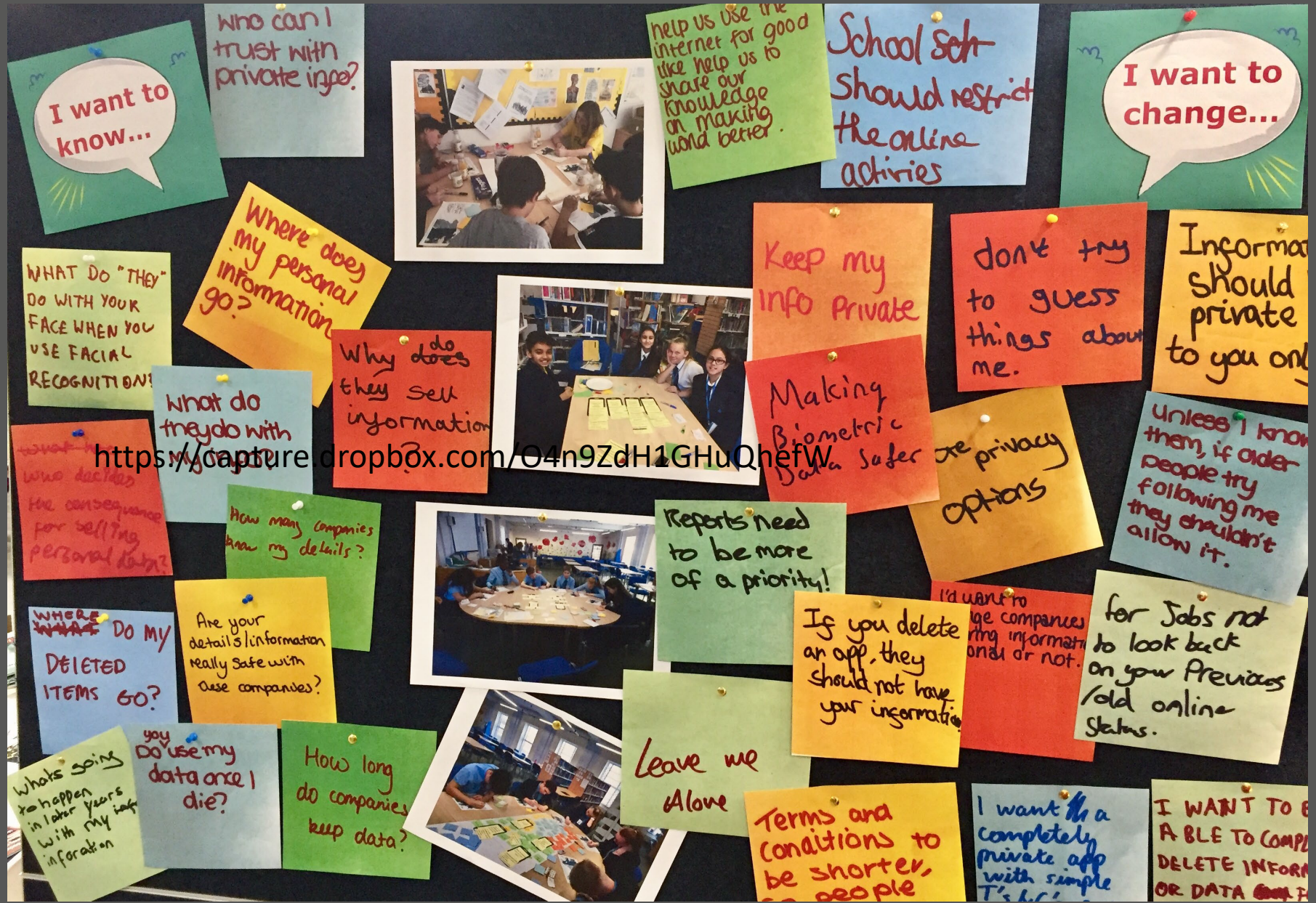
- Sites I visited
- Frequency of visits
- Adverts clicked

Sensitive information

- Religious or spiritual activities
- Body weight
- Your mental health

Preferences

- Films & music you like
- Food you eat
- Things you like to buy



<https://capture.dropbox.com/04n9ZdH1GHuQhefW>



My privacy

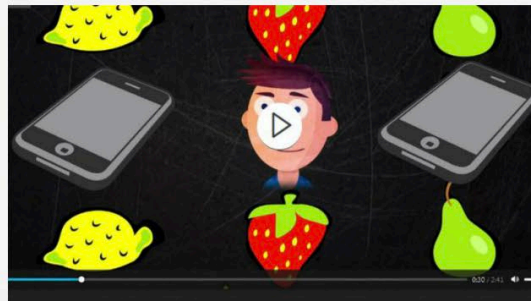
Well, we don't actually know where the information is going. You can sign up for an app and tell them your name and your age and stuff and they'll say at the bottom that it's all private and stuff, but then it goes somewhere. There's the question of where does it go.

boy, year 11, Midlands

Imagine that the internet knows everything about you! Does it matter if it does? What can you do to protect your privacy and data online?

We all use the internet a lot in our everyday life. We reveal a lot about ourselves online. And much of our data is being recorded and stored online by others (family, school, companies).

Watch our cartoon below to explain what this toolkit is all about.



It's only an online game, why read the small print? Thinking about privacy in a digital world

Print or share



For parents

For educators

For policy-makers

About



107. Digital forms of culture, recreation and play should support and benefit children and reflect and promote children's differing identities, in particular their cultural identities, languages and heritage... States parties should ensure that children have the opportunity to use their free time to experiment with information and communications technologies, express themselves and participate in cultural life online.

110. Leisure time spent in the digital environment may expose children to risks of harm, for example, through opaque or misleading advertising or highly persuasive or gambling-like design features. By introducing or using data protection, privacy-by-design and safety-by-design approaches and other regulatory measures, States parties should ensure that businesses do not target children using those or other techniques designed to prioritize commercial interests over those of the child.



What do you do just for fun?

For fun I would normally go on Netflix YouTube and social media's but one of the main things I do for fun is hang out with my family. It reminds me that there's a genuine reality rather than what I see online.



What fun can you have planning...

Tik tok and spending family tends to be... my play... communicate with... of Apps, games, or you to "just have fun" below.



What helps you to play with whatever you can find?

YouTube, is a good place to expand imagination such as you could paper near you and a YouTube video could pop up. But in a bro believe its instructions. We're b (education etc) to follow instru it makes it easier.

What helps you to play with whatever you can find?

Mouse-in-the-house is a game where you think of some where in your house and metaphorically hide a mouse there. Everyone else asks you questions to find out where the mouse is. Put your examples of Apps, games, or toys that let you "play with whatever you find" below.

Sewing Crafts

Sometimes we play...



"I always love having a cardboard box because I could draw all over it and it wouldn't matter."
(Girl, 12)

"It becomes its own sandbox environment ...it allows the imagination to go completely wild with it because it's not dealing with any constraints."
(Boy, 17)

"Each individual child will work out just exactly the potentiality of what that box could be."
(Theatre Professional)

"My five-year-old, he takes everything out of the box... and he will sit in the box and say, mama, I'm driving a car... It's quite interesting how they use their imagination in various ways ...to play and have fun."
(Mother)

To be 'Playful By Design', digital products and services should...

Be welcoming: Prioritise digital features that are inclusive, sociable and welcoming to all, reducing hateful communication and forms of exclusion and reflecting multiple identities.

Enhance imagination: Prioritise creative resources and imaginative, open-ended play over pre-determined pathways built on popularity metrics or driven by advertising or other commercial pressures.

Enable open-ended play: Provide and enhance features that offer easy-to use pathways, flexibility and variety as these support children's agency and encourage their imaginative, stimulating and open-ended play.

No commercial exploitation: Reduce compulsive features designed to prolong user engagement or cultivate dependency on games, apps or platforms, so children's immersive play is intrinsically motivated and freely chosen.

Ensure safety: Ensure children's play in online spaces is safe, including by giving them control over who can contact them and supplying help when needed.

Allow for experimentation: Recognise that exploration, invention and a degree of risk taking is vital in children's play and that the burden should not fall on them always to be cautious, anxious or follow rules set by others.

Be age-appropriate: Respect the needs of children of different ages by providing age-appropriate opportunities for play, while also allowing for safe intergenerational play.





**Convention on the
Rights of the Child**

Distr.: General
2 March 2021

Original: English

Committee on the Rights of the Child

**General comment No. 25 (2021) on children's rights in
relation to the digital environment**

B. Best interests of the child

12. The best interests of the child is a dynamic concept that requires an assessment appropriate to the specific context.⁵ The digital environment was not originally designed for children, yet it plays a significant role in children's lives. States parties should ensure that, in all actions regarding the provision, regulation, design, management and use of the digital environment, the best interests of every child is a primary consideration.



Designed with Kids in Mind

From apps that turn geolocation on for no reason and sneak in inappropriate ads, to platforms that offer confusing terms of service or introduce adult strangers to teens, too often digital services create unnecessary risks for kids.

These risks are just design choices. Apps and online platforms *can* be built in ways that reduce risks and increase safeguards for children instead. It's time to build an online world **designed with kids in mind.**

More than ever, we need a US design code to protect kids and teens online. **Will you join us?**

WRITERS

VIDEOS

BOOKS

LONG-READS

spiked

SHOP

The Online Safety Bill would treat us all like children

The UK government is actively encouraging Big Tech censorship.



LSE

Media and
Communications

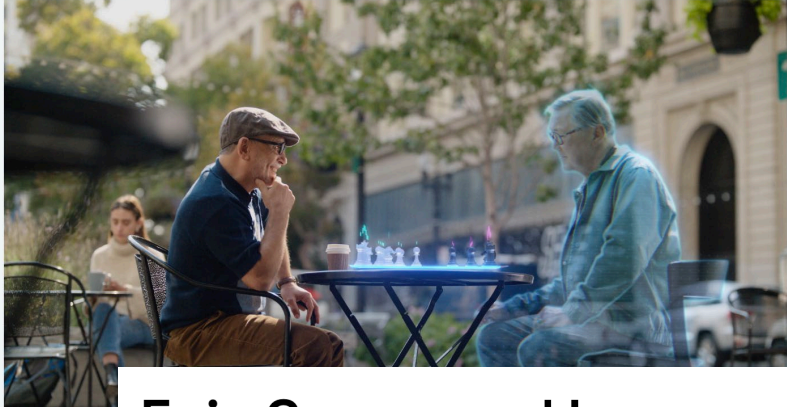


Nick Clegg

May 18 · 31 min read · Listen



Making the metaverse: What it is, how it will be built, and why it matters



Epic Games and Lego Partner up to Create a Kid-Friendly Metaverse

An 'exciting and playful future'

By [Lawrence Bonk](#) Published on April 7, 2022 11:49AM EDT

Fact checked by [Jerri Ledford](#)

[yahoo/finance](#) | Yahoo Finance UK

Metaverse gold-rush: The top five brands that are carving up the virtual space

Brian McGleenon

28 March 2022 · 11-min read

TRENDING

LSE

Media and Communications

Harassment and abuse in three dimensions, the dark side of the Metaverse

One digital watchdog was so shocked by the Metaverse footage which contained "abuse, harassment, racism and pornographic content", that they could not release it to The Feed, only describe it.

Published Sunday 20 March 2022

By Michelle Elias

Source: SBS



Peter Jukes
@peterjukes

A barrage of assault, racism and rape jokes: my nightmare trip into the metaverse

"Within 10 minutes, [the Guardian reporter] had witnessed the most disturbing sights of her life – in a space seven-year-olds can access"

Thanks Mark Zuckerberg



THE WALL STREET JOURNAL

SUBSCRIBE

SIGN IN

PRO CYBER NEWS

Come the Metaverse, Can Privacy Exist?

In immersive worlds, new technologies will siphon up data at an increasingly granular level—a person's gait, eye movements, emotions and more—putting far greater strain on existing safeguards



BROOKINGS



REPORT

A whole new world: Education meets the metaverse

Kathy Hirsh-Pasek, Jennifer M. Zosh, Helen Shwe Hadani, Roberta Michnick Golinkoff, Kevin Clark, Chip Donohue, and Ellen Wartella
Monday, February 14, 2022



