5Rights' Submission on Privacy and Children to the Special Rapporteur on the right to privacy

September 2020

Introduction

One in three global internet users are children,[1] with two children going online for the very first time every second.[2] Despite mediating almost all aspects of a young person's life, digital services are not designed with young people in mind and repeatedly fail to uphold the rights or safety of the young people who use them. This includes the right to privacy, to which children are entitled in accordance with Article 16 of the UN Convention on the Rights of the Child.[3]

The discourse about young people and the digital world is plagued by false binaries. For example, the right to privacy is frequently pitted against the right to freedom of expression[4] in discussions of child online safety, without recognition that young people are entitled to a digital environment that upholds both of these rights. One of the more telling enforcements of this binary is found in the debate over Facebook's plans to implement end-to-end encryption across all of its platforms,[5] where curtailing provisions to ensure young people's safety is framed as a regretful but necessary price to ensure privacy. This false binary will always result in an impasse and fail to ensure that CSAM[6] and grooming can still be detected. This has incomparable effects on children's rights – not just on their right to privacy.

Threats to privacy for young people in the digital environment are baked into design decisions including; a failure to provide high privacy settings on platforms of services young people use; wholesale harvesting of children's data; and the commercial usage of young people's data for the purposes of behavioural advertising, profiling, and algorithmic recommending.

The UN Convention on the Rights of the Child (UNCRC) was drafted 30 years ago, the same year as the invention of the world wide web, but to date these two 'worlds' have failed to recognise each other. For young people to realise their rights, they must be able to realise them in all contexts – including the digital. The digital environment should also be such where young people can enjoy the full gamut of their rights. 5Rights is currently supporting the UN Committee on the Rights of the Child to develop a general comment on Children's Rights in relation to the Digital World[7], including their right to privacy online. The general comment on the UNCRC will be an authoritative interpretation of how children's rights should be promoted and upheld in the digital environment and the digital age. This will provide a framework against which signatories to the UNCRC will be able to report how effectively they have upheld children's rights in relation to the digital environment.[8]

---

[1] UNICEF, One in Three: Internet Governance and Children's Rights, Sonia Livingstone, John Carr and Jasmina Byrne. January 2016.
[2] PwC and SuperAwesome, Kids digital media report 2019.
[3] UNCRC, Article 16
[4] UNCRC, Article 13
[5] Mark Zuckerberg, A Privacy-Focused Vision for Social Networking, March 2019.
[6] Where CSAM stands for Child Sexual Abuse Material, to accurately reflect 'the sexual abuse and exploitation of children.' This acronym is used by organisations such as National Center for Missing & Exploited Children (NCMEC), Barnardo's, and INHOPE.
[7] UNCRC/C/GC, 13 August 2020.
[8] The draft comment will be open for consultation until 15th November.

Below 5Rights Foundation outlines five areas relating to the privacy rights of children in the digital environment particularly with consideration of online social, recreational and educational spheres.

A lack of high-privacy default settings

Privacy settings allow users to control a range of features such as the visibility of their profile, who is allowed to contact or interact with them and their content, and what data a user consents to sharing with a service.

Online users overwhelmingly stick with the privacy and safety settings that they're given by default.[9] Default settings are often set to the lowest bar for privacy, in tandem with maximising opportunities for data collection. When users do choose to change these privacy settings, they are often met with unnecessary barriers and constraints, which makes it arduous to maintain high privacy. A 2019 article by CNET on default settings for privacy highlights that a "some assembly required" model for privacy settings is not an effective model for users to protect their data. It details the following:

> Privolta, a company that specializes in privacy-focused ads, ran a study in August and found that it takes 17 clicks to opt out of Google's data collection in the United Kingdom, while it only took one click to give the tech giant consent to collect your data. The company looked at 50 of the UK's top websites and found that, on average, it would take five times as long to opt out as it did to opt in for data collection.
> "It's designed to wear you down. That's how these patterns work," said Henry Lau, Privolta's co-founder." They don't want you to make an easy choice between yes and no, they just want you to visit the menu to review your options."[10]

Many young people do not have the maturity or skills to navigate privacy settings. Higher privacy settings are even *more* important for young people as they face unique risks due to their development stage and vulnerabilities associated with their age. Young people have repeatedly called on companies to make accounts private by default and describe confusion and frustration when trying to navigate privacy settings, particularly when trying to keep up with app updates.[11]

> *"Set high privacy settings from the start. We can turn them off if we want." – Participant from Royal Foundation Taskforce Focus Group.*

> *"Every website should make it mandatory to start your account as private and then you can decide to make what public whenever you want. Um, I think that's really important because most people, once they've signed up to a website, they forget to have a look at it. They forget to go back onto their settings, they just use it. So if it starts as private then the people who want to make it public will make the effort to, but the people who forget at least they'll be safe and they won't be getting any problems." – Participant from Youth Juries.*

> *"They deliberately make it as difficult as possible [to change settings]" – Participant from Youth Leader, Snap session.*

---

[9] Markus Tschersich and Reinhardt A. Botha, Understanding the Impact of Default privacy Settings on Self-Disclosure in Social Network Services, August 2013.
[10] CNET, Default settings for privacy – we need to talk, December 2019.
[11] Stoilova, M., Livingstone, S. and Nandagiri, R. (2019) Children's data and privacy online: Growing up in a digital age. Research findings. London: London School of Economics and Political Science. P.40

Among the effects of privacy settings, is that they make young people's profiles public by default.[12] These settings also allow adult strangers to send private messages to young people[13] or can allow strangers to watch livestreams from young people, often from intimate settings such as their bedroom[14]. Fundamentally, there must be more consideration of how features of online platforms contribute to privacy risks for young people and whether privacy settings are proportionate to a young person's age or capacity.

The Ask: High privacy settings by default

High privacy settings, by design and by default, would mitigate many of the risks young people currently face. For example, the UK has introduced the Age Appropriate Design Code,[15] a ground-breaking piece of legislation that, with its 15 provisions, recognises that young people require a necessarily higher bar of data protection that matches their developmental needs. In offering a higher standard of protection for young people's data, the UK government has taken an important step in transforming young people's online experience and safeguarding their right to privacy.

The Code's provision on default settings states that 'settings must be 'high privacy' by default, where providing young people with default high-privacy and safety settings offers a systemic way of reducing unnecessary risk. The Code's provisions cover default settings for interpersonal data (e.g. visibility of personal data to other users), data processing (e.g. what data does the platform collect and store to suggest in-app purchases) and for third-parties (e.g. what data is shared with advertisers to inform behavioural advertising), of which the latter two will be discussed in later sections.

When young people try to lower their privacy, the Code requires warning pop-ups to explain likely risks. Additionally, settings that support privacy and safely, for example those that restrict users' access to sensitive content, or give users additional, pop-up safety information should be *on by default* for young people.

Where risk can be mitigated by the implementation of high-privacy settings, what must remain, however, is that the norm of privacy must not mean responsibilisation[16] on young people. Young people have unique developmental vulnerabilities and evolving capacity, and therefore should not be placed with the burden of responsibility to manage their privacy settings, especially when evidence[17] suggests that platforms overwhelm users when they try to navigate their privacy settings.

A high bar of default privacy settings as a stand-alone provision, or an addendum to existing data protection legislation, is necessary to protect the privacy of young people under the age of 18.

Threats to privacy via data collection and storage

The enormous and ever-expansive digital footprint can easily curtail a young person's right to privacy when there is no knowledge or control over their data that is collected, stored, and shared. In some instances, it is not just a lack of knowledge or control, but it is explicitly going against

[12] For example, Instagram sets users profile as public by default when registering.
[13] Although it appears in the form of a "message request" when users receive a private message from someone they do not follow, strangers are still allowed to send private messages to children by default.
[14] NSPCC, Livestreaming and video-chatting, Snapshot 2.
[15] ICO, Age appropriate design: a code of practice for online services, September 2020.
[16] Professor Dr Eva Lievens, The Rights of the Child in the Digital Environment: From Empowerment to De-Responsibilisation, June 2020
[17] CNET, Default settings for privacy – we need to talk, December 2019.

consent altogether, such as the case of Google continuing to track their users, even after they have opted out of specific tracking settings.[18] SuperAwesome estimates that by the time a child is 13, adtech companies collect an average of 72 million data points on each young person in the digital.[19] This is still a conservative number, excluding embedded trackers used by Facebook, Twitter, and YouTube.

The culture of datafication and being *datafied* from birth, as defined by the notion of mass collection of data that is then shared within a lucrative global data ecology,[20] is a risk to young people's privacy. Existing legislation does little to secure young people's data protection in the digital environment if they are under-enforced.

The Ask: Enforce existing protections on young people's data

Children are afforded specific protection in relation to their data. GDPR-Kids, referring to the various provisions of the EU's General Data Protection Regulations (GDPR) that relate to children, for example, states: "Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.[21] This is in line with the Data Protection Act (2018) – the UK's implementation of the GDPR and the Age Appropriate Design Code.

Many ongoing cases against YouTube,[22] Google for Education,[23] Amazon,[24] and TikTok[25] concerning manipulative and illegal collection of young people's data, show that it is an industry norm to collect this data, despite all of the regulatory frameworks in place. Even though some of these data privacy cases are in the US, the EU and UK's own data protection laws mandate special protections that young people's data requires.

The provision of specific data protection for young people's data must be accompanied by enforcement of its terms, where a right to privacy cannot be realised unless and until existing data protection is vigorously enforced.

Threats to privacy over data misuse and profiling

Profiling,[26] and tracking users across platforms, is the norm for young people's experience of the digital environment. The commercial incentive for young people's data means that children are tracked, profiled, and bid on by advertisers for the opportunity to be advertised on. Even where young people have navigated privacy settings, and understood and made changes to these settings to reduce the type or amount of data collected by services, services may still deliberately and

[18] Forbes, Google Still Tracks App Users When They've Opted Out, Privacy Lawsuit Alleges, July 2020.
[19] SuperAwesome, How much data do adtech companies collect on kids before they turn 13? December 2017.
[20] Professor Sonia Livingstone OBE, "It's None of Their Business!" Children's Understanding of Privacy in the Platform Society, June 2020.
[21] GDPR, Recital 38.
[22] BBC, YouTube faces legal battle over British children's privacy, September 2020.
[23] New York Times, New Mexico Sues Google Over Children's Privacy Violations, February 2020.
[24] BBC, Amazon sued over Alexa child recordings in US, June 2019.
[25] The Verge, TikTok's parent company sued for collecting data on kids, December 2019.
[26] Profiling is defined in the GDPR as "any form of automated processing of personal data consisting the use of person data to evaluate certain aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour location or movements."

misleadingly 'track' users, such as the case of Google Chrome's deceptively un-private 'Incognito Mode.'[27] This cannot be said to uphold young people's right to privacy in any meaningful sense.

The increased use of algorithmic recommender systems[28] is a threat to young people's privacy in the digital environment. Because these systems are based on a model of ever-increasing data collection[29], young people face privacy risks from having their profiles served up to stranger adults through features such as Facebook's 'People You May Know.'[30]

The unintended consequences of data profiling and content recommendation can also pose a substantial risk to young people's privacy, particularly for sexual minorities. Over the years, there have been multiple reports of 'algorithmic outing', with Netflix reportedly tailoring home screen images to emphasise LGBTI content[31] and Facebook displaying advertising for LGBTI spaces[32] and "coming out" coaches.[33] Where these recommendations are inadvertently visible to other members of a household – through shared accounts or screens in communal rooms, for instance – the challenges for LGBTI young people are clear.

Most recently, the UK saw the devastating results of algorithmic decision making gone wrong via exam results[34]. Ofqual's decision to utilise an algorithm to determine exam results touches on Recital 71 of the GDPR, which stipulates that automated decision-making based solely on automated processing, including profiling, "should not concern" a child. This is a clear example of algorithmic decision-making to deny young people agency and control over important outcomes, and yet this is an industry norm.

In addition to algorithmic recommending, young people's data has been used to target users via behavioural advertising. Young people already struggle to recognise paid-for content[35] and are disproportionately susceptible to the pressures of advertising due to their developmental capacities.[36] The rights-based implications of behavioural advertising make it so that it is completely inappropriate to target young people via their data. There is both a lack of transparency of how a service's algorithm is used to recommend content to young people and a denial of young people's access to bespoke services in the digital environment.

The Ask: Protection of young people from profiling

Young people are afforded protections from being profiled by their data under both the Age Appropriate Design Code and the UNCRC. For example, algorithmically recommending news sources and heavily filtering the content young people receive can restrict a young person's right to access a variety of information under Article 17, and behavioural advertising seeking to influence,

---

[27] Elena Maris, Timothy Libert, and Jennifer Henrichsen, Tracking sex: The implications of widespread sexual data leakage and tracking on porn websites, Cornell University, July 2019.
[28] S.C. Olhede and P.J. Wolfe, The growing ubiquity of algorithms in society: implications, impacts and innovations, August 2018.
[29] Jennifer Cobbe and Jatinder Singh, Regulating Recommending: Motivations, Considerations, and Principles, *European Journal of Law and Technology*, April 2019.
[30] WIRED, Why does Facebook recommend friends I've never met? May 2019.
[31] Men's Health, Netflix's Algorithm Just Nearly Outed a Gay Teenager, November 2019.
[32] Into, Facebook Ads Outed Me, May 2018.
[33] Buzzdfeed News, Facebook Knew I Was Gay Before My Family Did, March 2013.
[34] BBC, A-levels and GCSEs: How did the exam algorithm work? August 2020
[35] LSE Department of Media and Communications, YouTube's child viewers may struggle to recognise adverts in videos from 'virtual play dates', September 2019.
[36] European Commission, Study on the impact of marketing through social media, online games and mobile applications on children's behaviour, March 2016.

manipulate, and direct behaviour infringes upon a young person's right to free play, rest, and leisure under Article 31.

The Code's provision on profiling says the option for features using profiling should be 'off 'by default for young people.[37] Profiling as "on" by default may only be allowed if a service has a compelling reason in line with a child's best interest, and has the appropriate measures in place to protect the child from harmful effects.

In order for services to switch profiling "off" by default, along with other data protection measures, a service must be able to demonstrate to a reasonably degree which of their users is a child. Robust and privacy-preserving age verification (or age assurance) in accordance with the level of risk a service posed to a young person will ensure that less content is directly fed to children based on their data, and that adults aren't inappropriately introduced to children as is currently the case.[38]

Profiling of young people's data must be in their best interests and restricted to those things necessary from the point of view of the child, not the service, platform, or product provider.

Threats to privacy via the rise of Ed-Tech, 'smart,' and connected products

The market for connected toys, wearable technology geared towards children,[39] and ed-tech is growing, especially in the context of the Covid-19 pandemic where a staggering 1.2 billion children are out of the classroom.[40] More than ever, young people are having to rely on the digital to permeate almost every facet of their lives.

In the UK, the growing dependence on ed-tech can be seen in the Department for Education's April 2020 proposal to provide laptops and tablets to disadvantaged children across England to 'make remote education accessible.'[41] This is despite the systemic risks laptops and ed-tech can have to young people's privacy, including the mining of "identifying" data from young people's voice clips[42] and being subject to CSEA imagery through 'zoombombing' video call hacking.[43]

As a result of the covid-19 pandemic, young people are completely reliant on digital technology for education. A lack of choice over how young people choose to attend school undermines their independence and can further exacerbate the digital divide. Where the UK government have failed to provide infrastructure for certain communities, young people are having to share devices[44] to attend lessons and thus face a significant threat to their data privacy in the digital environment.

The ICO's Age Appropriate Design Code stipulates explicit protections for children's data for products such as connected toys,[45] requiring effective tools embedded at the design level to adhere to the standards of the code.

---

[37] ICO, Profiling, Age appropriate design code, September 2020.
[38] Hobbies, interests, and other factors are used by friend suggestions systems to algorithmically match users. A recent investigation found that adult predators adopting similar interests to children were being steered towards children's accounts, including those as young as 11, on popular social media platforms. To read more: Risky by Design, 5Rights Foundation.
[39] WIRED, All the clues suggest the new Apple Watch will be aimed at children, May 2020
[40] World Economic Forum, The Covid-19 pandemic has changed education forever. This is how, April 2020.
[41] Department for Education, New major package to support online learning, April 2020.
[42] Telegraph, 'Virtual classes' over video apps could place children at risk, school warns, March 2020.
[43] Independent, 60 young people subject to footage of child abuse after Zoom call hacked, May 2020.
[44] BBC, Digital divide: Six children sharing one phone for homework, July 2020.
[45] ICO, Connected toys and devices, Age appropriate design code.

However, young people's right to privacy is not just impacted by these specific products, and the growth of smart home products means that young people are likely to encounter these products in their daily life, but there is very little consideration to the specific protections to privacy young people require. In 2015, just over 25% of broadband households with children at home owned at least one smart home device. 5 years later, the average UK home now has 10.3 internet-enabled devices, rising to an average of 15.4 items when children are in the household.[46]

Many of these connected devices have been shown to not been designed with the particular needs and vulnerabilities of young people in mind, leaving their right to privacy undermined by making them at risk from contact by stranger adults,[47] or collecting and processing of their speech data.[48] As Barassi and Scanlon (2020) write, data traced collection through speech recognition can have a profound impact on children's rights by virtue of profiling and classifying young people on a group-level which may reproduce existing inequalities and impact individual rights to self-definition and autonomy.[49]

The Ask: Privacy by Design for 'smart', connected, and Ed-Tech products

It would be prudent to conduct child impact assessments so that the privacy risks facing young people online are anticipated and mitigated *before* products and services are distributed, and on an on-going basis.

Impact assessments are a common and established means of identifying the future consequences of a current or proposed action. Under the Data Protection Act[17] and the statutory Age Appropriate Design Code,[18] a Data Protection Impact Assessment (DPIA) must be carried out to assess and mitigate any risks to the rights and freedoms of young people arising from data processing. This must be done before processing any high-risk data and if the DPIA identifies any high risks which cannot be mitigated, then the Information Commissioner must be consulted before any data is processed.

Data privacy for young people will not be realised until all of the products or services they are likely to access conduct impact assessments on their collection, storage, and usage of young people's data.

Threats to privacy from incomprehensible published terms

All of the aforementioned requirements and protections for young people's data should be visible in published terms, where they are clear to children and enforced. *Published terms* normally consist of at least three separate documents: community standards or guidelines, terms and conditions, and a privacy notice. For data privacy, published terms represent a crucial opportunity for digital platforms and services to communicate with young people the expectations of data collection that the service requires. Published terms are at the heart of setting out an agreement between the service and a young person, allowing young people and their parents to understand[50] the nature of an online service and anticipate the risks it might pose. Recital 58 of the GDPR mandates the need for age-appropriate language for information and communication for processing of children's data. It is not

[46] Aviva, Tech Nation: number of internet-connected devices grows to 10 per home, January 2020.
[47] Independent, Children could be contact by strangers through cameras and microphones on smart toys, Which? finds, December 2019.
[48] Dr. Veronica Barassi and Dr. Patricia Scanlon, Voice Prints and Children's Rights, May 2019.
[49] *Ibid.*
[50] ICO, Policies and community standards, Age Appropriate Design Code.

possible for a young person to exercise their right to privacy over their data if platforms deny this important communication with young users.

The industry norm of manipulative data collection practices means that currently published terms are mostly incomprehensible[51] for a young person, rarely read, and poorly upheld. If young people do not know what terms and conditions are saying, they are disempowered from making informed choices to 'agree' to published terms, undermining their autonomy.

Some services provide intentionally opaque published terms, using nudge techniques or dark patterns to persuade users to agree to more aggressive data collection practices.[52] This may not be meaningful consent to a service's intended data collection practices.

The Ask: Age appropriate published terms are upheld and enforced

Several principles of the Age Appropriate Design Code are dedicated to published terms, highlighting the importance of these terms to obtain meaningful consent from young people regarding their data. These provisions include Policies and community standards,[53] Transparency,[54] and Nudge techniques.[55]

Systemic changes to the culture of young people's data collection is the way forward to build a digital ecosystem that upholds their right to privacy. Part of this change means that data collection practices are transparent and understood by young people at the start of their digital journeys[56] and are upheld through to the services and products they use.

Conclusion

It will never be possible to protect children's privacy until the following measures are enforced: a high bar of default privacy settings as a stand-alone provision; specific protections for young people's data; profiling of young people's data only in their best interests and as necessary, rather than for the commercial incentive for a service or product provider; child impact assessments including the usage of young people's data; and age appropriate published terms including young people's data collection practices.

Upholding children's right to privacy means enforcing the aforementioned measures and implementing systemic changes at the design level by doing 'privacy by design.' These are already mandated by frameworks such as GDPR, DPA and most recently AADC. Only when these existing legislative frameworks are enforced, can young people's right to privacy be realised in the digital environment.

---

[51] VICE News, Most Online 'Terms of Service' are Incomprehensible to Adults, February 2019; New York Times, We Read 150 Privacy Policies: They Were An Incomprehensible Disaster.

[52] Forbruker Rådet, Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy, June 2018.

[53] ICO, Policies and community standards, Age Appropriate Design Code.

[54] ICO, Transparency, Age Appropriate Design Code

[55] ICO, Nudge techniques, Age Appropriate Design Code

[56] Since November 2019, 5Rights Foundation has been supporting the Institute of Electrical and Electronics Engineers (IEEE) Working Group to create standard P2089 to help digital service providers measure their own published terms and determine whether or not they are age appropriate. By providing a standard for age appropriate published terms, P2089 identifies the need for realising children's rights in the digital by ensuring that these rights, and especially the right to privacy, is embedded within the design of digital products and services that young people access and are impacted by.

For further information please contact 5Rights Researcher Manpreet Singh at manpreet@5rightsfoundation.com

About 5Rights Foundation

5Rights Foundation develops new policy, creates innovative projects and challenges received narratives, to ensure governments, regulators, the tech sector and society understand, recognise and prioritise young people's needs and rights in the digital world. Our work has been widely understood to be pragmatic and implementable as we work with governments, intergovernmental institutions, professional associations, academics and young people across the globe to build the digital world that young people deserve.