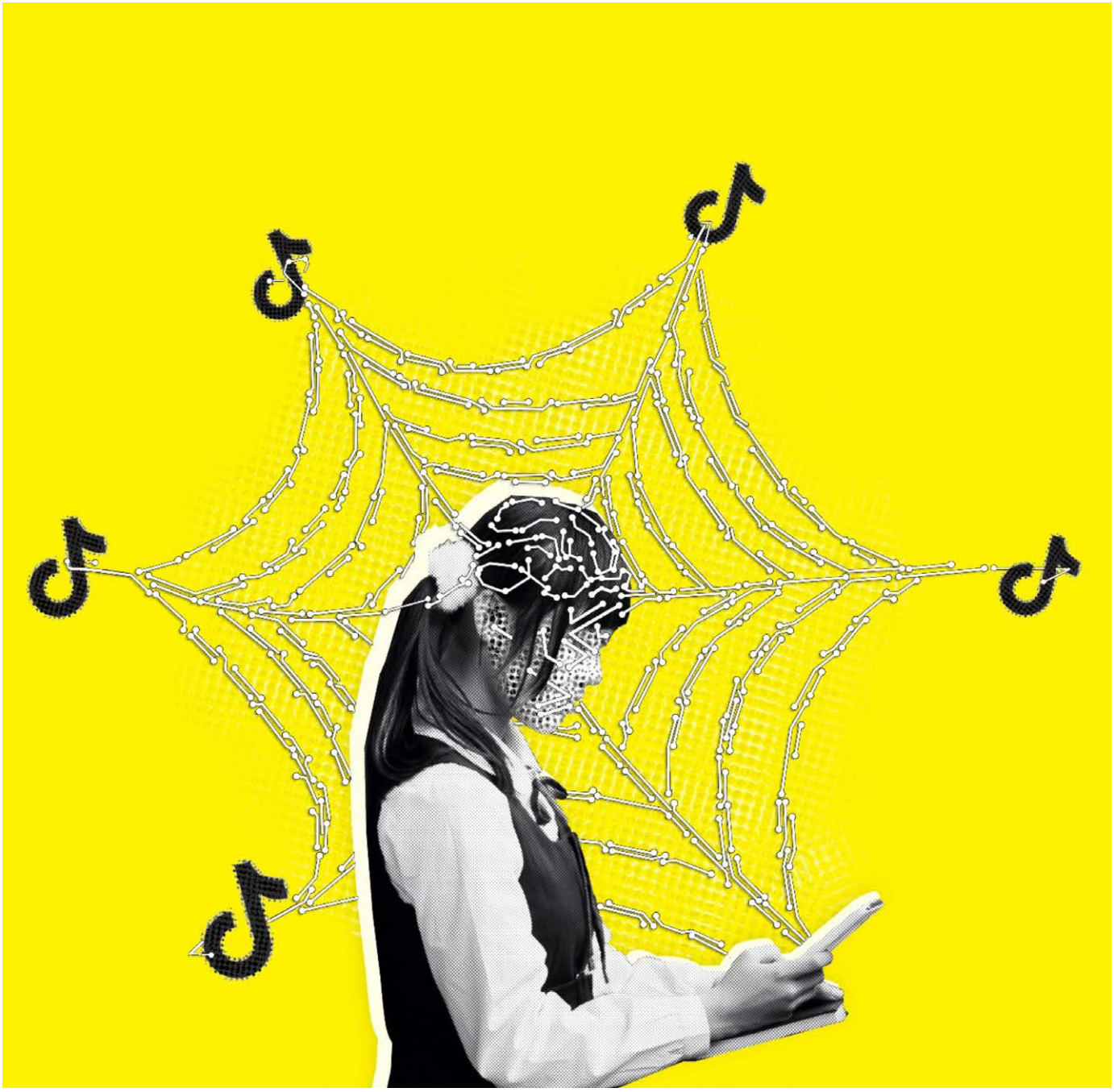


“I FEEL EXPOSED”

CAUGHT IN TIKTOK’S SURVEILLANCE WEB

AMNESTY INTERNATIONAL

Amnesty International is a movement of 10 million people which mobilizes the humanity in everyone and campaigns for change so we can all enjoy our human rights. Our vision is of a world where those in power keep their promises, respect international law and are held to account. We are independent of any government, political ideology, economic interest or religion and are funded mainly by our membership and individual donations. We believe that acting in solidarity and compassion with people everywhere can change our societies for the better.

First published in 2023
by Amnesty International Ltd
Peter Benenson House, 1 Easton Street,
London WC1X 0DW, UK

Index: POL 40/7350/2023
Original language: English

amnesty.org

Credit Luisa Balaban.

AMNESTY INTERNATIONAL

CONTENTS

GLOSSARY

Algorithms	An algorithm is a procedure used for solving a problem or performing a computation. Algorithms act as an exact list of instructions that conduct specified actions step by step, typically used to solve specific problems or to perform a computation. Algorithms are used as specifications for performing calculations and data processing. "Algorithmic systems" are applications that perform one or more tasks such as gathering, combining, cleaning, sorting, classifying and inferring data, as well as selection, prioritization, making recommendations and decision-making.
Artificial Intelligence or AI	There is no widely accepted definition of the term "artificial intelligence" or "AI". The United Nations (UN) Office of the High Commissioner for Human Rights (OHCHR) uses the term to refer to a constellation of processes and technologies enabling computers to complement or replace specific tasks otherwise performed by humans, such as making decisions and solving problems, including machine learning and deep learning.[1]
CAADCA	California Age-Appropriate Design Code Act
CCPA	California Consumer Privacy Act
CJEU	Court of Justice of the European Union
Content moderation	"Content moderation" refers to social media platforms' oversight and enforcement of platform rules in relation to permissible and prohibited forms of expression. It can include actions such as the detection, demotion and removal of content which violates platform rules.
COPPA	(USA) Children's Online Privacy Protection Act
CRC	Convention on the Rights of the Child
DPA	Data Protection Authority
DPIA	Data protection impact assessment
DPC	(Irish) Data Protection Commission
DSA	(EU) Digital Services Act
DDPA	Dutch Data Protection Authority
ECtHR	European Court of Human Rights
FTC	(US) Federal Trade Commission
GDPR	General Data Protection Regulation

1. UN High Commissioner for Human Rights, Report: *The Right to Privacy in the Digital Age*, 15 September 2021, UN Doc. A/HRC/48/31, footnote 2.

Global Majority	"Global majority" is a collective term for ethnic groups which constitute approximately 85 percent of the global population.
HRC	UN Human Rights Committee
ICCPR	International Covenant on Civil and Political Rights
ICERD	International Convention on the Elimination of All Forms of Racial Discrimination
ICO	(UK) Information Commissioner's Office
Nudges	Nudge Theory or the concept of nudging was popularized by behavioural economist Richard Thaler and legal scholar Cass Sunstein in their book *Nudge: Improving Decisions About Health, Wealth and Happiness* (2008). Nudge Theory posits that adaptations to the design used to present choices can influence the behaviour and decision-making of groups or individuals. A nudge, according to Thaler and Sunstein, is "any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any option or significantly changing their economic incentive."[2]
Machine Learning	The use and development of computer systems that are able to learn and adapt without following explicit instructions, by using algorithms and statistical models to analyse and draw inferences from patterns in data.
OECD	Organisation for Economic Co-operation and Development
OECD GUIDELINES	OECD Guidelines for Multinational Enterprises
OHCHR	Office of the High Commissioner for Human Rights
Recommender System	Algorithmic recommender systems are information filtering systems, whose purpose is to suggest items that are most relevant or of greatest interest to a particular user. They do this by ranking, prioritizing and amplifying certain messages. They are responsible for what kind of content people see in their social media feeds. As such, they influence public discourse and affect people's ability to retrieve and interact with information online.
UDHR	Universal Declaration of Human Rights
UK GDPR	(UK) General Data Protection Regulation
UN guiding principles	UN Guiding Principles on Business and Human Rights
VLOP	Very large online platform (as designated by the European Commission)
VLOSE	Very large online search engine (as designated by the European Commission)

2. Richard Thaler and Cass Sunstein, *Nudge: Improving Decisions About Health, Wealth and Happiness*, 2008; Ana Caraban and others, "23 Ways to Nudge: A Review of Technology-Mediated Nudging in Human-Computer Interaction", Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, May 2019, Paper No. 503, https://dl.acm.org/doi/10.1145/3290605.3300733

1. EXECUTIVE SUMMARY

Dance-craze videos, challenges, cooking recipes, lip-syncing videos. TikTok can be a rich source of creative content, where users can discover new things and find communities. In the space of only a few years, this has helped it become one of the biggest social media companies in the world, with over 1 billion users, many of whom are children between the ages of 13 and 17. But behind the infinitely scrollable feed of lip-syncing and dance choreography videos is a highly extractive business model that fundamentally undermines human rights.

This business model is based on the collection of massive amounts of personal data on each user's behaviour. TikTok then uses this data to create profiles of users and draw inferences about them, which allows it to cluster users in groups to target them with highly personalized content. These groups are also made available to advertisers to allow them to target them with personalized ads.

Central to TikTok's success, and a defining part of the TikTok user experience, is its 'For You' page, the default user experience, which is a feed powered by an algorithmic recommender system that delivers personalized content that is likely to be of interest to the specific user. The 'For You' feed is often portrayed as the most sophisticated result of the trend towards ever more hyper-personalized feeds, where users only need to watch recommended content for certain amounts of time for the system of algorithms to gauge the user's interests, match these with the available video content and serve up more personalized recommendations and advertisements. The 'For You' feed is optimised to predict, with apparently startling accuracy, which content will appeal to an individual user and keep them engaged on the platform, thus facilitating the collection of ever more data.

This report builds on Amnesty International's 2019 report, *Surveillance Giants*, which highlighted the way in which the abuse of the right to privacy is at the heart of the surveillance-based business model employed by Big Tech companies, particularly leading social media platforms. This model is based on the massive collection, storage, analysis, and ultimate exploitation of data relating to users who are tracked across the web, through the apps on their phones, and in the physical world. These companies collect extensive data on what we search, where we go, who we talk to, what we say and what we read. Through analysis made possible by machine learning, they can infer our moods, ethnicities, sexual orientation, political opinions, and vulnerabilities among other things. Some of these characteristics – including characteristics protected under human rights law – are then made available to others for the purpose of targeting internet users with advertisements.

The real-life consequences of the surveillance-based business model on the physical and mental health of children and young people are set out by Amnesty International in the companion to this report, *Driven into Darkness: How TikTok encourages self-harm and suicide ideation*. This report explores the risks that TikTok poses to the physical and mental health of children and young people, particularly for those already experiencing mental health concerns. It reveals the way in which TikTok's

algorithmic recommender system exposes children and young people to serious health risks, through a design that turns their psychological vulnerabilities into a way to maximize their engagement with the platform and profit for the company. In this way, TikTok risks exposing a young person experiencing depressive symptoms to a social media feed consisting of a high volume of posts that discuss, normalize, or even romanticize depressive thinking, self-harm, and suicide, which has the potential to exacerbate young users' pre-existing mental health issues and can potentially contribute to harmful and even devastating real-world actions.

This report is based on research conducted by Amnesty International between September 2022 and October 2023 into the privacy and advertising policies and practices of the social media platform TikTok as they relate to users that are under the age of 18.

In order to seek further information about TikTok's policies regarding users under the age of 18 and its due diligence processes Amnesty International sent written questions to TikTok, as well as a letter laying out the findings in this report and inviting TikTok to respond. TikTok did not agree with all of the findings. Their full responses can be found in Annex II.

In addition, the report draws on a survey carried out by the organization in the form of an online questionnaire, distributed via Amnesty International and partner organizations' social media channels and responded to by 550 children and young adults between the ages of 13 and 24 in 45 countries in October and November 2022. The questionnaire asked about use of leading social media platforms and experiences on these platforms with a view to better understand lived experiences, concerns and attitudes towards social media.

Amnesty International's analysis of the surveillance-based business model sets out the relevant international human rights framework relating to the rights to privacy, freedom of thought, freedom of opinion and non-discrimination, and how they are affected by the surveillance-based business model used by social media companies, including TikTok. It also looks at the specific protections to which children are entitled under international law and outlines key measures that should be taken by states to ensure that social media companies' operations respect children's rights and best interests as recommended by United Nations (UN) treaty bodies and experts.

Amnesty International's analysis shows how the surveillance-based business model represents an intrusion into billions of people's private lives that can never be necessary or proportionate. Social media companies, including TikTok, have made access to their services conditional on users 'consenting' to the processing and sometimes (depending on a user's location) the sharing of their personal data for marketing and advertising, directly countering the right established in many countries' data protection legislation to decide when and how our personal data can be shared with others.

Research with children aged between 11 and 16 however has shown that they often fail to grasp the consequences of privacy violations taking place at scale. Further research has shown that the terms and conditions of the most popular social media platforms are not easily accessible or understandable by children aged between 13 and 17. As "Ella", 17, from Norway wrote in Amnesty International's survey:

> ***"It feels very invasive and like they know everything about me. In a way I feel exposed.***
>
> ***I try to read them [terms of service] whenever I sign up for anything but they're very hard to read through so I end up just scanning through all of it without really understanding it."***

This means that any consent granted by children and young people cannot be considered genuinely free and informed, which directly impacts their ability to have control over their own information.

Finally, the companies' use of algorithmic systems to create and infer detailed profiles on people interferes with children's ability to shape their own identities within a private sphere. This is particularly

important when considering the evolving capacities of children who are growing, developing, and trying out new identities all the time.

The surveillance-based business model of many social media companies, including TikTok, undermines each of the three elements of the right to privacy to such an extent that it undermines the very essence of privacy.

And, as with the right to privacy, the surveillance-based business model, on which TikTok and other social media platforms base their businesses, has implications for all three elements of the right to freedom of thought, but in particular the first element – the right to keep your thoughts and opinions private.

Social media companies can also undermine the right to non-discrimination through various practices, including by the way in which content and advertisements are targeted, through the amplification of content which discriminates against a particular category of persons or community, and/or through the application of policies in a discriminatory manner. For instance, social media companies risk abusing the right to non-discrimination through their ad practices and the categories that they offer in order to enable advertisers to target selected users.

The report finds that with technology developing at an ever-faster pace, lawmakers and regulatory efforts around the world are struggling to keep up. There has been little progress towards addressing the systemic risks associated with large social media platforms, and to date few states or regional organizations have adopted legislation.

Among the few jurisdictions that have taken action is the European Union, whose Digital Service Act, adopted in July 2022, became the first major regional-level "Big Tech" regulation, aimed at limiting the harmful effects of social media platforms, including by banning intrusive "targeted advertising" towards children.

While the introduction of a ban on targeted advertising to children under 18 in Europe is a step in the right direction and will create more privacy-respecting experiences for teen users, research has found that "the best way to keep children safe from the sale of their personal data on the internet is to ban all online advertising which targets users based on personal data".

As a result of a growing awareness of the risks posed by social media to the right to privacy, particularly for children, there is mounting public concern and pressure, which has resulted in an increasing number of investigations by data protection authorities into the misuse of data, including that of children in some jurisdictions. TikTok has not been immune to this sort of regulatory action and there have been a number of important cases concerning its privacy and data collection policies and practices relating to children, which have resulted in fines.

To assess whether TikTok is respecting child users' rights on the platform, this report reviews TikTok's privacy policies and other publicly available documents related to data collection and advertising practices. TikTok's policy is divided into three regions: European Economic Area (EEA)/United Kingdom (UK)/Switzerland, United States and Other Regions. The three policies are broadly similar but have several important differences, which means that the level of protection to children's privacy differs depending on the region in which they live.

TikTok collects a huge amount of data on each user, tracking them on the app and collecting data on their activity on the wider internet, as well as in the physical world as well (for example through approximate location data or in-store purchase data shared by partners), which many users will not realise they are agreeing to when they sign-up for an account. The direct and indirect collection of this massive amount of data is a clear abuse of the right to privacy. TikTok then uses this data to infer a

user's attributes and interests. Certain interest categories can overlap with or reveal sensitive personal information or can be used as proxies for protected characteristics and be used to target people or exclude them. For instance, people interested in baby products, who are likely to be expectant parents, including pregnant women and birthing people, may be targeted with baby-related content, or excluded from seeing other adverts, or people signalling an interest in LBGTI+ content could be taken as proxy for their sexuality. The inferring of user charateristics and interests involves an abuse of the right to freedom of thought, specifically the right to not reveal one's thoughts.

Furthermore, comparing TikTok's three privacy policies and the data collected under each one reveals key differences particularly with respect to how much data is collected from users under in the EEA/Switzerland/UK and those subject to the Other Regions policy, which creates a discriminatory patchwork of policies. This is particularly troubling, as in many parts of the world the data of children over the age of 13 is treated the same as adults' data.

All companies have a responsibility to respect all human rights wherever they operate in the world and throughout their operations. To fulfil its responsibilities as laid out in the UN Guiding Principles on Business and Human Rights, TikTok therefore should be conducting appropriate human rights due diligence to identify, prevent, mitigate and account for how it is addressing its potential and actual harms. As part of this human rights due diligence, the company should have identified the risks to children and young people inherent in the design of its platform, its data collection practices and algorithmic recommender system. In its response to Amnesty International's findings, TikTok failed to disclose any specific risks that it had identified. Importantly, TikTok also disclosed that it is currently developing a company-wide human rights due diligence process, revealing that it does not have one. TikTok is thus failing to carry out adequate human rights due diligence in line with international standards and thus is failing in its responsibility to respect human rights, as laid out in the UN Guiding Principles.

The failure of TikTok to put in place adequate policies to respect the rights of children makes it clear that stronger laws and regulation on data protection and algorithmic amplification of content on social media, and effective enforcement of such laws and regulation, are needed in order to keep children safe from the harvesting and exploitation of their personal data for profit. Governments around the world need to urgently make further and faster progress towards protecting people from the systemic risks related to social media companies' business model by taking effective measures to prevent, investigate, punish, and provide redress for abuses through effective policies, legislation, regulations and adjudication in line with international human rights law and standards.

It also requires a complete transformation of the business model on which TikTok, and other social media companies, have built their businesses. The internet does not need to depend on mass surveillance. Indeed, the widescale abuses of rights to privacy and freedom of thought and opinion are not inherent to online services. Rather, they arise from deliberate design decisions which are aimed at enabling TikTok to grow its user base and profits.

1.1 KEY RECOMMENDATIONS

TO TIKTOK

Amnesty International calls on TikTok to urgently implement the following recommendations:

- TikTok should immediately stop allowing advertisers to target children around the world under the age 18 with personalized ads based on their on and off-TikTok activity, as it has done in the European Economic Area, the UK and Switzerland.

- Transition to a rights-respecting business model that is not based on invasive data tracking. As a first step, TikTok must ensure that its human rights due diligence policies and processes address the systemic and widespread human rights impacts of its business model, in particular the right to privacy, the right to freedom of thought and the right to health.
- TikTok must stop maximizing "user engagement" at the expense of its users' health and other human rights. As part of its human rights due diligence process, TikTok must identify design elements in cooperation with users, including children and young people, and independent experts, which encourage addictive platform use and social comparison, and replace these with a user experience that is focused on 'safety by design' and the best interests of the child.
- To respect privacy and to provide users with real choice and control, a profiling-free social media ecosystem should not just be an option but the norm. Content-shaping algorithms used by TikTok and other online platforms should therefore not be based on profiling (for example, based on watch time or engagement) by default and must require an opt-in instead of an opt-out, with the consent for opting in being freely given, specific, informed (including using child-friendly language) and unambiguous.
- TikTok must cease collecting intimate personal data and drawing inferences from a user's watch time and engagement about their interests, emotional state or well-being for the purposes of 'personalizing' content recommendations and ad targeting. Rather than using pervasive surveillance to adapt feeds to a user's interests, TikTok should enable users to communicate their interests through deliberate prompts (for example, users could be asked to enter specific interests if they would like to be served personalized recommendations) and only when based on users' freely given, specific and informed consent.

TO STATES

To fulfil children's rights, states must:

- Prevent companies from making access to their service conditional on individuals 'consenting' to the collection, processing or sharing of their users' personal data for content targeting and marketing or advertising.
- Regulate social media companies to ensure that content-shaping algorithms used by online platforms are not based on profiling by default and that they require an opt-in rather than an opt-out, with the consent for opting in being freely given, specific, informed and unambiguous. The collection and use of inferred data (for example, recommendations based on watch time and likes) to personalize ads and content recommendations should be banned. Rather, users should be in control of which signals or declared interests they want the platform to factor into the shaping of their feed. For those who prefer a feed based on personalized recommendations, they must be given the option to communicate personal interests to the platform based on specific, freely given and informed consent and based on prompts made in child-friendly language.
- Ensure that independent national data protection regulators are established, that their independence is guaranteed in law and that they have adequate resources, expertise and powers to meaningfully investigate and sanction abuses of regulations by social media companies in line with international human rights law and standards. They must be able to ensure independent and effective oversight over platform design as well as the design, development and implementation of algorithmic systems to ensure companies are held legally accountable for the identification, prevention and mitigation of human rights harms linked to such systems.
- Require by law that technology companies carry out ongoing and proactive human rights due diligence to identify and address human rights risks and impacts related to their global operations,

including those linked to their algorithmic systems or arising from their business model as a whole. Where businesses target children or have children as end users, they should be required to integrate child rights into their due diligence processes, in particular to carry out and make publicly available child rights impact assessments, with special consideration given to the differentiated and at times severe impacts of the digital environment on children. They should take appropriate steps to prevent, monitor, investigate and punish child rights abuses by businesses.

2. METHODOLOGY

This report is based on research conducted by Amnesty International between September 2022 and September 2023 into the privacy and advertising policies and practices of the social media platform TikTok as they relate to users that are under the age of 18.[3] In particular, the research examines whether and how TikTok's surveillance-based business model undermines children's rights to privacy and freedom of thought and opinion, and how levels of protection differ according to the geographic regions in which young users live.

The report focuses on TikTok because it is one of the fastest growing social media platforms with more than 1 billion active users,[4] the majority of whom are thought to be children and young people.[5]

The research was carried out by Amnesty International researchers with the support of an external independent consultant, who conducted an initial analysis of the terms of service, privacy and advertising policies of TikTok, as well as other relevant company documents. This was complemented by a further in-depth review by Amnesty International researchers of TikTok policies and other publicly available information on its policies and practices. Amnesty International researchers reviewed TikTok's three regional privacy policies covering the European Economic Area (EEA)/United Kingdom (UK)/Switzerland[6] (last updated on 4 May 2023) the US[7] (last updated on 22 May 2023) and 'Other Regions'[8] (last updated on 4 August 2023). Amnesty International researchers also conducted additional desk research using information from open sources, including publications by UN experts, civil society organizations, academics, as well as media sources.

In order to seek further information about TikTok's policies regarding users under the age of 18 and its due diligence processes Amnesty International sent written questions to TikTok. TikTok's written responses to these questions, received on the 12 July 2023, are reflected in this report and a full copy is attached in Annex II. In accordance with Amnesty International's policy of providing targets the right

3. Amnesty International defines a child as anyone under the age of 18 years in line with the UN Convention on the Rights of the Child (CRC).
4. TikTok Newsroom, "Thanks a billion!", https://newsroom.tiktok.com/en-gb/1-billion-people-on-tiktok-uk; Reuters, "TikTok's ad revenue to surpass Twitter and Snapchat combined in 2022", 11 April 2022, https://www.reuters.com/technology/tiktoks-ad-revenue-surpass-twitter-snapchat-combined-2022-report-2022-04-11/; Statista, "TikTok users worldwide 2027", 23 August 2023, https://www.statista.com/forecasts/1142687/tiktok-users-worldwide
5. Reliable global figures for the number of TikTok users between 13 and 17 do not exist, but a recent report by the Pew Research Center found that 67% of all teens (aged 13-17) in the US use TikTok, reflecting the high levels of usage in this age group. Pew Research Center, "Teens and Social Media: Key findings from Pew Research Center Surveys", 24 April 2023, https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/, p.12. According to the Ofcom study, half of children in the UK aged between 3-17 years old used TikTok in 2021, making it the third most-used platform overall. Ofcom, *Children and Parents: Media Use and Attitudes Report 2022, 30 March 2022*, https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-and-parents-media-use-and-attitudes-report-2022, p.25. Meltwater, "54 TikTok stats you need to know [2023]", 30 December 2022, https://www.meltwater.com/en/blog/tiktok-statistics; Guardian, "What TikTok does to your mental health: 'It's embarrassing we know so little'", 30 October 2022, https://www.theguardian.com/technology/2022/oct/30/tiktok-mental-health-social-media; Reuters Institute for the Study of Journalism, Reuters Institute , "Digital News Report 2023" (previously cited).
6. TikTok, Privacy Policy (EEA/UK/Switzerland) (updated 4 May 2023), https://www.tiktok.com/legal/page/eea/privacy-policy/en
7. TikTok, Privacy Policy (United States) (updated 22 May 2023), https://www.tiktok.com/legal/page/us/privacy-policy/en
8. TikTok, Privacy Policy (Other Regions), https://www.tiktok.com/legal/page/row/privacy-policy/en (updated on 4 August 2023).

to reply, the organisation wrote to TikTok on 12 October 2023 laying out our findings and inviting TikTok to respond. TikTok's responses to Amnesty International's conclusions, received on 29 October 2023, are also reflected in the report where relevant and their response is attached in Annex II.

In addition, the report draws on a survey carried out by Amnesty International in the form of an online questionnaire,[9] distributed via Amnesty International and partner organizations' social media channels and responded to by 550 children and young adults between the ages of 13 and 24 in 45 countries in October and November 2022. The questionnaire asked about use of leading social media platforms, experiences on these platforms, likes and dislikes, reactions to negative experiences and visions for change, with a view to better understand lived experiences, concerns and attitudes towards social media.[10] Quotations from children and young people who took part in the survey are featured in this report, although their names have been changed in order to protect their identity. The quotations express their perceptions and experiences of social media.

This report builds on a previous report by Amnesty International into the human rights implications of the surveillance-based business model of social media companies: *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights (Surveillance Giants)*.[11] It complements, and should be read in conjunction with, a new report, *Driven into Darkness: How TikTok encourages self-harm and suicide ideation (Driven into Darkness)*,[12] which explores the risks that TikTok poses to the physical and mental health of children and young people, particularly for those already experiencing mental health concerns.

9. Amnesty International, Survey on Children and Young People's Experiences on Social Media, (Index: POL 40/7355/2023), https://www.amnesty.org/en/documents/pol40/7355/2023/en/
10. Amnesty International, "'We are totally exposed': Young people share concerns about social media's impact on privacy and mental health in global survey", 7 February 2023, https://www.amnesty.org/en/latest/news/2023/02/children-young-people-social-media-survey-2
11. Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights* (Index: POL 30/1404/2019), 21 November 2019, https://www.amnesty.org/en/documents/pol30/1404/2019/en
12. Amnesty International, *Driven into Darkness: How TikTok encourages self-harm and suicide ideation*, (Index: POL 40/7350/2023), 7 November 2023, https://www.amnesty.org/en/documents/pol40/7350/2023/en/

3. BACKGROUND

> ***"It feels very invasive and like they know everything about me. In a way I feel exposed***
>
> ***I try to read them [terms of service] whenever I sign up for anything but they're very hard to read through so I end up just scanning through all of it without really understanding it."***
>
> "Ella", 17, Norway, 2022

> ***"Companies have access to everything we look at and post. Occasionally ads pop up on other social media platforms based on what I've looked at, which raises questions surrounding the security of our data."***
>
> "Freya",17, UK, 2022

3.1 THE GROWTH OF SOCIAL MEDIA

The internet and digital environment form an ever greater and more important part of children's lives today, whether they are connecting with friends and like-minded communities on social media, using education platforms to assist their learning, or accessing state and other services through automated processes. Digital technologies and the online environment provide children with a vast array of opportunities for growth, learning, experimenting and discovery. However, the digital environment, including social media platforms, was generally not designed with children in mind despite the important role it plays in their lives,[13] including massive numbers of under-18s that regularly use social media or have a presence online, with figures as high as 98% of all teens aged 12-17 in the UK[14] and

13. UN Committee on the Rights of the Child, General Comment 25: Children's Rights in Relation to the Digital Environment, 2 March 2021, UN Doc. CRC/C/GC/25, para. 12.
14. Ofcom, *Children and Parents: Media Use and Attitudes Report 2022,* 30 March 2022, https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-and-parents-media-use-and-attitudes-report-2022

95% of teens 13–17 in the US.[15] The use of social media has grown exponentially in recent years, with TikTok among the social media apps with the most users. According to TikTok, by September 2021 the platform had more than 1 billion active users.[16] Elsewhere, figures for social media use in general, and TikTok use in particular, show that these platforms play a huge role in people's lives, particularly for children and young people, who have never known a world without them.

Amnesty International's 2022 survey of children and young adults' experiences of and attitudes towards social media (see Chapter 2 "Methodology") found that TikTok and other social media platforms have become daily fixtures in their lives, with 59% of respondents spending more than two hours on average per day on social media.[17]

Although survey participants were positive about the diversity of content and ideas, the possibility for creativity and opportunities for activism they also had significant concerns. Chief among these was the toll on mental health of harmful content and "addictive" platform design, and feelings of powerlessness in the face of constant nudging by the apps to participate in a vicious cycle of personal data sharing and content consumption.

Survey participants also described a sense of lack of control in protecting their privacy. Three-quarters of the 550 respondents said that they found social media companies' terms of service hard to understand and were critical of the often "technical language" used in their policies and the take-it-or-leave-it approach which forces users to choose between conceding their privacy by signing-up to the platforms or risking exclusion from online public spaces and communities where their peers communicate, interact and exchange ideas.

3.2 THE SURVEILLANCE-BASED BUSINESS MODEL

> **"I think it's so scary how they collect it [personal information] and save it, how it could possibly be used against you. How companies sell your data so that others may know more about you to make more money off of you."** 17, "Hennie", Norway, 2022

> **"The amount of personal information they have about me that I am probably not even aware that they have, how algorithms can be scare [sic] in the way they only show you stuff that align with you and your beliefs / values / interests, something that can lead to brainwashing."** 18, "Leo", Norway, 2022

Amnesty International's 2019 report, *Surveillance Giants* highlighted the way in which the abuse of the right to privacy is at the heart of the surveillance-based business model employed by Big Tech companies, particularly social media platforms. This model is based on the massive collection, storage, analysis, and ultimate exploitation of data relating to users who are tracked across the web, through the apps on their phones, and in the physical world, as well through the expansion of the "Internet of Things" as they go about their daily activities.[18] Some apps for instance will track users and collect their approximate or precise location from their mobile device or allow users to "check-in" to locations and share it with their contacts. Other internet-enabled smart home devices such as TVs,

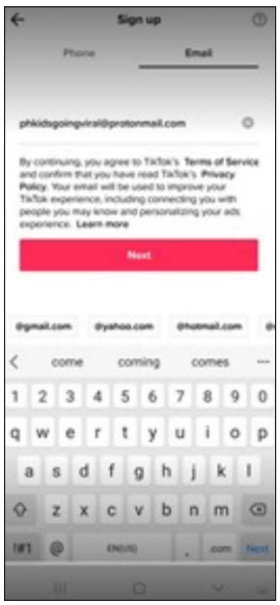
15. Pew Research Center, "Teens and Social Media: Key findings from Pew Research Center Surveys", 24 April 2023, https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/,
16. TikTok Newsroom, "Thanks a billion!", https://newsroom.tiktok.com/en-gb/1-billion-people-on-tiktok-uk; Reuters, "TikTok's ad revenue to surpass Twitter and Snapchat combined in 2022", 11 April 2022, https://www.reuters.com/technology/tiktoks-ad-revenue-surpass-twitter-snapchat-combined-2022-report-2022-04-11/
17. Amnesty International, "'We are totally exposed': Young people share concerns about social media's impact on privacy and mental health in global survey" (previously cited).2)
18. Amnesty International, *Surveillance Giants* (previously cited).

doorbells, heating system thermostats etc. may also collect data on users that is aggregated with other personal data.[19]

In summary, these companies collect extensive data on what we search, where we go, who we talk to, what we say and what we read. Through analysis made possible by machine learning, they can infer our moods, ethnicities, sexual orientation, political opinions, and vulnerabilities among other things. Some of these characteristics – including characteristics protected under human rights law – are then made available to others for the purpose of targeting internet users with advertisements.

Social media platforms also use "dark patterns",[20] referred to as "deceptive design",[21] to encourage users, including the many millions of children and young people around the world that use these platforms, to sign up to these services, agree to their terms of service and, in the process, give away or give access to huge amounts of personal data.

The term 'dark patterns' is used to describe "instances where designers use their knowledge of human behavior (e.g., psychology) and the desires of end users to implement deceptive functionality that is not in the user's best interest."[22]



Sign-up page for TikTok with the Next button in a bold bright colour while the link to the terms of service is small and in black.

The huge troves of data and the insights drawn from them are ultimately exploited for profit. Amnesty International's previous research showed how two of the social media giants, Meta and Google, have optimized the use of big data analytics and the addictive design of social media platforms so effectively that they have been able to dominate the world's advertising market,[23] sharing between them an estimated 48.4% of all global ad spending in 2022, though this is expected to drop to 44.9% by the end of 2023, as other platforms including TikTok continue to eat into their market share.[24]

The risks to privacy posed by the surveillance-based business model are well documented. Even when its foundations were being developed 20 years ago, privacy advocates warned of the dangers of individualized online profiling and the need for legal safeguards. Such warnings continued as the failure of social media companies to self-regulate became increasingly evident. For example, in 2000, the then Director of US-based research group, the Electronic Privacy Information Center, Marc Rotenburg, told the US Senate "We warned [a year ago] that self-regulation would fail to protect privacy and that there would be a public backlash against the company's [DoubleClick's][25] plan to profile Internet users."[26]

19. The Guardian, "How to stop your smart home spying on you | Smart homes", https://www.theguardian.com/technology/2020/mar/08/how-to-stop-your-smart-home-spying-on-you-lightbulbs-doorbell-ring-google-assistant-alexa-privacy ; Mozilla Foundation, "*privacy not included | Shop smart and safe", https://foundation.mozilla.org/en/privacynotincluded/ (accessed 16 October 2023)
20. Colin Gray and others, , "The dark (patterns) side of UX design", CHI, 2018, https://dl.acm.org/doi/pdf/10.1145/3173574.3174108 ;"Dark patterns tip line", https://darkpatternstipline.org/; "Deceptive patterns", https://www.deceptive.design/ (both accessed on 11 October 2023).
21. "Deceptive patterns" (previously cited).
22. Colin Gray and others, "The dark (patterns) side of UX design" (previously cited).
23. Amnesty International, *Surveillance Giants* (previously cited).
24. Search Engine Land, "Google and Meta are losing their edge as TikTok, Amazon, Instacart ads grow", 6 January 2023, https://searchengineland.com/google-and-meta-are-losing-their-edge-as-tiktok-amazon-instacart-ads-grow-391062
25. DoubleClick Inc. was an American advertisement company that developed and provided Internet ad serving services from 1995 until its acquisition by Google in March 2008.
26. Electronic Privacy Information Center, Testimony and Statement of Marc Rotenberg, Executive Director of the Electronic Privacy Information Center on Internet Privacy and Profiling to the US Senate Commerce Committee, 13 June 2000, https://www2.epic.org/privacy/internet/senate-testimony.html

The real-life consequences of this failure of self-regulation on the physical and mental health of children are set out in the companion to this report, *Driven into Darkness*. As Amnesty International's 2022 report, *Myanmar: The Social Atrocity – Meta and the Right to Remedy for the Rohingya (The Social Atrocity)*, also documented, this surveillance-based business model can also result in the amplification of extreme content that, in the case of Myanmar, incited violence, hatred and discrimination against the Rohingya people, ultimately contributing to the Myanmar security forces' ethnic cleansing and incitement of mass violence against Rohingya Muslims in 2017.[27] Amnesty International's 2023 report '*A death sentence for my father': Meta's contribution to human rights abuses in northern Ethiopia* (*'A death sentence for my father'*) shows how many of the same systemic failures that occurred in the context of Myanmar were repeated in Ethiopia. The report reveals the devastating impacts that the Facebook platform's engagement-based business model had in the context of Ethiopia's armed conflict and the serious human rights abuses perpetrated against the Tigrayan community between 2020 – 2022.[28]

3.3 WHAT IS TIKTOK?

TikTok is a short-form video hosting service and social media platform owned by Chinese technology company, ByteDance Ltd. In November 2017, ByteDance acquired Musical.ly, a social media platform on which users could create 15-second to one-minute lip-syncing music videos, choose soundtracks to accompany them, and edit them using different speed options, pre-set filters and effects. Musically was already popular among teenagers in the US, and by the end of May 2017 was reported to have more than 200 million users with half of all US teenagers using the platform.[29]

Following its acquisition by ByteDance, in August 2018 Musical.ly was absorbed into TikTok (which already existed as a similar platform) and all Musical.ly accounts were automatically migrated to TikTok.[30]

TikTok's global popularity grew dramatically during the Covid-19 lockdowns in 2020 and 2021, as people who were cut off from their usual social networks spent more time online. The number of active users on the platform was reported to have roughly doubled between December 2019 and September 2021.[31] Today, ByteDance claims that the TikTok platform, which is available outside China (although banned in India,[32] Jordan,[33] Somalia[34] and the US state of Montana[35]), is the leading short-form video platform,[36] reaching more than 1 billion active users in 2021[37] and, according to

27. Amnesty International, *Myanmar: The Social Atrocity – Meta and the Right to Remedy for the Rohingya* (Index: ASA 16/5933/2022), 29 September 2022, https://www.amnesty.org/en/documents/asa16/5933/2022/en/
28. Amnesty International, '*A death sentence for my father': Meta's contribution to human rights abuses in northern Ethiopia*, (Index: AFR 25/7292/2023), 31 October 2023, https://www.amnesty.org/en/documents/afr25/7292/2023/en/
29. Billboard, "Musical.ly, Apple Music Ink New Partnership, With More to Come", 28 April 2017, https://web.archive.org/web/20200306215031/https:/www.billboard.com/articles/business/7776302/musically-apple-music-partnership
30. ByteDance, "History of ByteDance", https://www.bytedance.com/en/ (accessed on 1 July 2023); Vox, TikTok, explained", 12 July 2019, https://www.vox.com/culture/2018/12/10/18129126/tiktok-app-musically-meme-cringe
31. We Are Social and Hootsuite, *Digital 2022 Global Overview Report*, 26 January 2022, https://wearesocial.com/hk/blog/2022/01/digital-2022-another-year-of-bumper-growth
32. Guardian, "India bans TikTok after Himalayan border clash with Chinese troops", 29 June 2020, https://www.theguardian.com/world/2020/jun/29/india-bans-tiktok-after-himalayan-border-clash-with-chinese-troops
33. Roya News, "Government clarifies potential TikTok return in Jordan", 24 August 2023, https://en.royanews.tv/news/44011/2023-08-24#:~:text=TikTok%20has%20been%20banned%20in%20Jordan%20since%20December
34. Al Jazeera, "Outcry in Somalia over government decision to ban TikTok, Telegram", 26 August 2023, https://www.aljazeera.com/news/2023/8/26/outcry-in-somalia-over-government-decision-to-ban-tiktok-telegram)
35. Mashable, "Montana legislature passes TikTok ban (Update: Ban is now law)", 17 May 2023, https://mashable.com/article/montana-tiktok-ban
36. ByteDance, "History of ByteDance" (previously cited).
37. TikTok Newsroom, "Thanks a billion!", https://newsroom.tiktok.com/en-gb/1-billion-people-on-tiktok-uk; Reuters, "TikTok's ad revenue to surpass Twitter and Snapchat combined in 2022", 11 April 2022, https://www.reuters.com/technology/tiktoks-ad-revenue-surpass-twitter-snapchat-combined-2022-report-2022-04-11/

separate reports, approximately 1.7 billion in 2022.[38] The majority of its users are thought to be children and young people.[39]

Central to TikTok's success, and a defining part of the TikTok user experience, is its 'For You' page, which predicts, with apparently startling accuracy, what content will appeal to an individual user and keep them engaged on the platform.[40] The 'For You' page is a feed powered by an algorithmic recommender system that delivers personalized content that is likely to be of interest to the specific user.

The tailoring of recommended content begins, when a user first opens the app and selects areas of interest. Even if no categories of interest are selected, TikTok's recommender system offers a feed of recent videos based on popular videos appropriate for a broad audience and influenced by the user's country and language settings.

Whether the user selects areas of interest or not, once they start engaging with content, the system begins to adjust their feed in response to inferred data based on their activity on the app (views, skips, likes, comments, shares etc.) to create a personalized 'For You' feed. The recommendations in the 'For You' feed are based on metrics, including user interactions (videos users like or share, accounts users follow etc.), video information (such as captions, sounds and hashtags) and device and account settings (such as language and country, though these are less influential to the rankings than other data points).[41]

According to TikTok, all these data points are processed by the algorithmic recommender system and weighted based on their value to the user. Metrics related to how long a user watches a particular video or whether a user finishes watching a particular video are considered strong indicators of interests and weighted more heavily than other factors. Videos are then ranked according to whether they are likely to be of interest to a user and are delivered to their 'For You' feed.[42] Predictions about suggested content are also influenced by the interactions of other users on TikTok who appear to have similar interests. So, for example: "if User A likes videos 1, 2, and 3 and User B likes videos 1, 2, 3, 4 and 5, the recommendation system may predict User A will also like videos 4 and 5."[43]

TikTok's 'For You' feed, the default user experience, is often portrayed as the most sophisticated result of the trend towards ever more hyper-personalized feeds, where users only need to watch recommended content for different amounts of time for the system of algorithms to gauge the user's interests, match these with the available video content and to serve up more personalized recommendations and advertisements. TikTok's algorithmic recommender system thus allows it to deliver a highly personalized experience for each user, which is optimized to keep them engaged online. This in turn allows TikTok to collect vast amounts of personal data, which TikTok can use both to target more personalized content at users and for some users, target them with personalized ads.

"I don't like that apps can track your info, I feel it so invasive [sic]."

20, "Valentina", Argentina, 2022

38. Statista, "TikTok users worldwide 2027", 23 August 2023, https://www.statista.com/forecasts/1142687/tiktok-users-worldwide
39. Pew Research Center, "Teens and Social Media: Key findings from Pew Research Center Surveys", 24 April 2023, https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/, p.12; Ofcom, *Children and Parents: Media Use and Attitudes Report 2022*, 30 March 2022, https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-and-parents-media-use-and-attitudes-report-2022, p.25. Meltwater, "54 TikTok stats you need to know [2023]", 30 December 2022, https://www.meltwater.com/en/blog/tiktok-statistics; Guardian, "What TikTok does to your mental health: 'It's embarrassing we know so little'", 30 October 2022, https://www.theguardian.com/technology/2022/oct/30/tiktok-mental-health-social-media; Reuters Institute for the Study of Journalism, Reuters Institute , "Digital News Report 2023" (previously cited).
40. The Cut, "How Does TikTok Know So Much About Me?", 22 July 2021, https://www.thecut.com/2021/07/tiktok-algorithm-knows-me.html
41. TikTok, "How TikTok recommends content", https://support.tiktok.com/en/using-tiktok/exploring-videos/how-tiktok-recommends-content; TikTok, "How TikTok recommends videos #ForYou", 18 June 2020, nhttps://newsroom.tiktok.com/en-us/how-tiktok-recommends-videos-for-you (both accessed on 1 July 2023).
42. TikTok, "How TikTok recommends videos #ForYou" (previously cited).
43. TikTok, "How TikTok recommends content" (previously cited).

3.4 ONLINE ADVERTISING AND HOW TIKTOK USES IT

Social media has changed the landscape of advertising. Through its collection of massive amounts of data on individual users, it has become possible to target individuals with highly personalized adverts. Academics have defined three types of online targeted advertising:[44]

- **Explicit targeted advertising**, which is based on matching the targeting criteria for an ad with personal information and data collected when users create a social media account, such as age, gender, location, relationship status, school or education provider, employer, friends etc. This data is then used by advertisers or ad delivery systems to target ads based on the information that users have explicitly and knowingly entered on their profiles.
- **Individual personalized targeting mechanisms** that in addition to the personal attributes and interests shared and specified by the users in their profile, are also based on predicted characteristics and information. By aggregating all the information about a user's online activity (posts, likes, comments, location etc.), social media companies are able to use machine learning and data analysis algorithms to predict additional personal information in a user's profile. These predicted attributes can then be used to target users with even more personalized adverts. Because this predictive targeting is based on inferences drawn from information about behaviour both on and offline it expands the targeting criteria available to social media companies and advertisers to include often highly sensitive information that a user would not have chosen to divulge, such as their sexual orientation, credit score or medical conditions.
- **Lookalike targeting** or targeting of **lookalike audiences** (also referred to as affinity profiling or affinity audiences) in which advertisers or businesses upload information on existing audiences of relevant users that are already known to the advertiser or brand – for example, because they are previous customers or have already engaged with the brand or business online. An algorithm is then used to generate a "lookalike audience" of users that are similar to the original source audience. While lookalike audiences change the model so that advertisers do not specify a list of attributes or interests that they want to use to target users, the algorithm creates the lookalike audience by making predictions about personal attributes, common interests, and information, some of which will be sensitive, for those within the lookalike audience. This model thus still has the same implications for human rights as targeted personalized advertising.

All three models have implications for the right to privacy. Explicit targeted advertising impacts on the right to privacy the least, as in theory the ads that people are shown respond to data that the user has explicitly and knowingly shared. Both individual personalized targeting mechanisms and lookalike audiences involve an abuse of the right to privacy because inferences are drawn about users' personal characteristics and interests that the user has not divulged. Furthermore, they impact on the right to freedom of thought, particularly the right to keep your thoughts private. These impacts are discussed more in Chapter 4.

TikTok makes all three types of advertising available to businesses and like other social media platforms makes its money through a combination of advertising revenue and, more recently, e-commerce. It uses the same model of highly personalized content to deliver ads and sponsored content tailored to individual users as it does to deliver the personalized content to 'For You' feeds.

44. Rainer Mühlhoff and Theresa Willem, "Social media advertising for clinical studies: Ethical and data protection implications of online targeting", 21 February 2023, Big Data & Society, Volume 10, Issue 1, https://journals.sagepub.com/doi/10.1177/20539517231156127

This growth in advertising revenue is reinforced by TikTok's encouragement to advertisers "to embrace" TikTok's style and tone and to fit in with the platform and its community of users.[45] Its "Don't make ads. Make TikToks" campaign exhorts advertisers to create content such as full-screen videos using songs and sound of the type that users are used to engaging with. TikTok also connects brands with influencers and in some cases works with companies to help them create content and viral challenges that are designed to reach millions of users according to the information gathered on their profiles and preferences.

TikTok is also moving into e-commerce. In 2023, it launched an in-app marketplace called TikTok Shop,[46] which "enables merchants and creators to showcase and sell products for the TikTok community to discover and purchase directly through a complete in-app experience."[47] Again, TikTok Shop is highly personalized as it is designed so that users can move directly from live streams and short videos showcasing products and brands, which users may have discovered through the highly personalized 'For You' feed to an the in-app shopping site, thus creating a closed loop with TikTok handling every step from a user seeing a product to buying it.

This business model of amassing ever more data on users to make finely tuned and precise predictions about their likes, wants and interests and making this information available for advertisers to use to target them with ads, or using it to direct users to creators who sell products in the in-app marketplace TikTok Shop is crucial to TikTok's success and profitability. However, as set out below, the model is inherently abusive to the rights to privacy and freedom of thought.

45. TikTok, "What we mean when we say 'Don't Make Ads", 6 September 2021, https://www.tiktok.com/business/en-US/blog/what-we-mean-when-we-say-dont-make-ads
46. TikTok Shop has launched in the UK, US and Saudi Arabia, as well as Southeast Asia, where it reportedly shows the strongest growth. Tech Wire Asia, E-commerce platforms: what's behind the rise of TikTok Shop?, 24 August 2023, https://techwireasia.com/2023/08/can-tiktok-shop-reign-over-e-commerce-platforms-in-southeast-asia/ Tech Crunch, "TikTok Shop officially launches in the US", 12 September 2023, https://techcrunch.com/2023/09/12/tiktok-shop-officially-launches-in-the-u-s/
47. TikTok Shop, "TikTokShop" https://shop.tiktok.com/business/en (accessed on 1 July 2023).

4. APPLICABLE HUMAN RIGHTS FRAMEWORK AND CONCERNS RELATING TO SOCIAL MEDIA

> ***"I think many people know that their data is being used to optimize the algorithm. The algorithm is what scares me the most I guess because it has the power to encourage extremism. I'm also concerned about the fact that social media companies are not only using the data I actively choose to share but also analyse every little passive thing I do."***
>
> 17, "Sofia", Germany, 2022

This chapter sets out the international human rights framework relating to rights to privacy, freedom of thought, freedom of opinion and non-discrimination, and how they are affected by the surveillance-based business model of social media companies, including TikTok. It also looks at the specific protections to which children are entitled under international law and outlines key measures that should be taken by states to ensure that social media companies' operations respect children's rights and best interests as recommended by United Nations (UN) treaty bodies and experts.

The right to health, another right that is fundamental to children and their well-being, is addressed in the companion report, *Driven into Darkness*, which explores the way in which TikTok's algorithmic recommender system exposes children and young people to serious health risks, through a design that turns their psychological vulnerabilities into a way to maximize their engagement with the platform and profit for the company. *Driven into Darkness* shows how TikTok risks exposing a young person experiencing depressive symptoms to a social media feed consisting of a high volume of posts that discuss, normalize or even romanticize depressive thinking, self-harm and suicide, which has the potential to exacerbate young users' pre-existing mental health issues and can potentially contribute to harmful and even devastating real-world actions.

4.1 THE RIGHT TO PRIVACY

The right to privacy is protected under international and regional[48] human rights instruments, including Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR) which provide that no one should be subject to "arbitrary or unlawful interference" with their privacy, family, home or correspondence, and this should be protected by law.[49] Children's right to privacy is expressly protected under Article 16 of the Convention on the Rights of the Child (CRC).

The UN Human Rights Committee (HRC), the body responsible for monitoring the implementation of the ICCPR by states parties, has long recognized that such protection includes regulating "the gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies."[50]

The need for evolving understandings of the scope of the right to privacy in response to the development of new technologies is also recognized, particularly in the digital environment. The UN High Commissioner for Human Rights has stated that:

"Privacy can be considered as the presumption that individuals should have an area of autonomous development, interaction, and liberty, a 'private sphere' with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals. In the digital environment, informational privacy, covering information that exists or can be derived about a person and her or his life and the decisions based on that information, is of particular importance."[51]

The High Commissioner has further emphasised the broad scope of the right to privacy, noting that it is not limited to private, secluded spaces, such as a person's home, but also "…extends to public spaces and information that is publicly available."[52]

THE THREE ELEMENTS OF THE RIGHT TO PRIVACY

The right to privacy encompasses three inter-related concepts:

- the freedom from intrusion into our private lives;
- the right to control information about ourselves;
- the right to a space in which we can freely express our identities.

Intrusion into private lives is only permissible under international human rights law if it is neither arbitrary nor unlawful. Human rights mechanisms have consistently interpreted this as referring to the overarching principles of legality, necessity and proportionality.[53]

The UN High Commissioner for Human Rights has noted that protection of the right to privacy extends not only to the content of communications but also to metadata as, when analysed and aggregated, such data "may give an insight into an individual's behaviour, social relationship, private preference and identity that go beyond even that conveyed by accessing the content of a communication."[54] The

48. At the regional level, the right to privacy is protected by: Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and Article 11 of the American Convention on Human Rights.
49. UDHR, Article 12; ICCPR, Article 17.
50. HRC, General Comment 16: The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (Article 17), UN Doc. HRI/GEN/1/Rev.9 (Vol. I), 8 April 1988, para. 10.
51. UN High Commissioner for Human Rights, Report: *The Right to Privacy in the Digital Age*, 3 August 2018, UN Doc. A/HRC/39/29, para. 5.
52. UN High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, 3 August 2018, (previously cited), para. 6.
53. Office of the High Commissioner for Human Rights (OHCHR), *The Right to Privacy in the Digital Age*, 30 June 2014, UN Doc. A/HRC/27/37, paras 21-27.
54. UN High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, 3 August 2018, (previously cited), para. 6.

High Commissioner has further noted that "even the mere generation and collection of data relating to a person's identity, family or life already affects the right to privacy, as through those steps an individual loses some control over information that could put his or her privacy at risk."[55]

A 2016 UN General Assembly resolution on the right to privacy, raised concerns about the risks to the enjoyment of the right to privacy in the digital age by the increasing capabilities of business enterprises to collect, process and use personal data.[56] It emphasized the corporate responsibility to respect human rights and called on states to develop and enforce adequate legislation that protects individuals against violations and abuses of the right to privacy through the unlawful and arbitrary collection, processing, retention or use of personal data by businesses. It further called on companies to inform users about the collection, use, sharing and retention of their data and to establish transparency policies.[57]

The right to control personal information or the right to "informational self-determination",[58] entails being able to decide when and how our personal data can be shared with others.[59] An individual's ability to control personal information is the foundation for data protection measures, which have become increasingly important since the advance of large-scale databases and associated computational technologies.

European Court of Human Rights (ECtHR) rulings have recognized that the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to privacy,[60] and that privacy provides for the right to a form of informational self-determination.[61]

However social media companies, including TikTok, have made access to their services conditional on users 'consenting' to the processing and sometimes (depending on a user's location) the sharing of their personal data for marketing and advertising, directly countering the right established in many countries' data protection legislation to decide when and how our personal data can be shared with others.

Furthermore, while children may tick the boxes to say they agree to this harvesting of their data, research with children aged between 11 and 16 has shown that although they place great value on the protection of their privacy and dignity in the digital realm, they fail to grasp the consequences of privacy violations taking place at scale, instead focusing on their own perceived agency and the responsibility of friends and family, rather than corporations.[62]

A 2021 audit of terms and conditions of ten of the most popular social media platforms, including TikTok, and exploration of whether children between the ages of 13-17 could reasonably understand them by an Australian non-governmental organisation (NGO), found that, although the terms and conditions varied, none were easily accessible or understandable by children aged between 13 and 17.[63]

---

55. UN High Commissioner for Human Rights, *The Right to Privacy in the Digital Age*, 3 August 2018, (previously cited (previously cited), para. 7.
56. UN General Assembly (UNGA), Resolution 71/199: The Right to Privacy in the Digital Age, adopted on 19 December 2016, UN Doc. A/RES/71/199
57. UNGA, Resolution 71/199: The Right to Privacy in the Digital Age (previously cited), para. 6(b).
58. The term "informational self-determination" was first used in the context of a German Constitutional Court ruling relating to personal information collecting during the 1983 census. The Court ruled that it is the authority of the individual to decide when and within what restrictions information about their private life should be communicated to others. BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983 - 1 BvR 209/83 -, Rn. 1-215, https://www.bverfg.de/e/rs19831215_1bvr020983.html
59. Alan Westin, *Privacy and Freedom*, 1967.
60. S and Marper v UK, Applications nos. 30562/04 and 30566/04, European Court of Human Rights (ECtHR), 4 December 2008 available at http://hudoc.echr.coe.int/eng?i=001-90051.
61. Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, Application no. 931/13, ECtHR, 27 June 2017, at para.137, available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-175121%22]}.
62. Stoilova, Livingstone and Nandagiri. *Media and Communication*, 8 (4), 2020. *Digital by default: children's capacity to understand and manage online data and privacy* 197 - 207. ISSN 2183-2439; Lapenta and Jorgensen, *View of Youth, privacy and online media: Framing the right to privacy in public policy-making, First Monday*, Volume 20, Number 3 - 2 March 2015, http://dx.doi.org/10.5210/fm.v20i3.5568
63. Reset Australia, *Did We Really Consent to This? Terms & Conditions and Young People's Data*, July 2021, https://au.reset.tech/uploads/l01_resettechaustralia_policymemo_t_c_report_final-july.pdf

"I usually read the Terms of Service, and I feel pressured by other people to skip it. This because one have to agree either way. I like to know what I consent for. It is hard to understand everything. And it is hard to read all of it. One does not remember all of it 4 days later." "Olli", 16, Norway, 2022

Legal scholars and subject experts have repeatedly criticized the "click-wrap"' nature of these "contracts"' that users, including children and young people, commonly accept without reading. The impossibility of reading, let alone absorbing, the terms and conditions of such contracts has been highlighted in the past by academics in, who in 2008 found that "a reasonable reading of all the privacy policies one encounters in a year would require 76 full workdays".[64] The use of these "dark patterns" (described in Chapter 3.1) and the difficulty of reading and understanding the terms of service means that any consent granted by children and young people cannot be considered to be genuinely free and informed consent. The opaqueness of these terms of service impact on the right to privacy, as they directly impact a user's ability to have control over their own information.

Finally, ***the space to construct our own identities*** is also intrinsic to the right to privacy and is based on an understanding that an individual's sense of identity is both socially constructed, relational and dynamic: we show different sides of our personalities in different contexts, be it with our friends, at work or in public, and this is constantly shifting, adapting and responding to our environment.[65]

Privacy enables us to decide for ourselves how others see us – and we behave differently when we are subjected to unwanted observation. In this sense, privacy is essential for autonomy and the ability to of individuals to determine their own identity. This is particularly important when considering the evolving capacities of children who are growing, developing, and trying out new identities all the time.

The surveillance-based business model of many social media companies undermines each of the three elements of the right to privacy discussed above to such an extent that it undermines the very essence of privacy.

The form of mass corporate surveillance used by social media companies, including TikTok, represents an unnecessary and disproportionate intrusion into private lives and is therefore inconsistent with the right to privacy. As a comparison, where states have claimed that indiscriminate mass surveillance is necessary to protect national security, human rights mechanisms have stated that this practice "is not permissible under international human rights law, as an individualized necessity and proportionality analysis would not be possible in the context of such measures."[66] Additionally, by making access to their platforms conditional on users "consenting" to the collection, processing and sometimes (depending on a user's location) the sharing of their personal data for marketing and advertising, social media companies also undermine users' ability to control when and how their personal data can be shared with others.

Furthermore, social media platforms such as TikTok have become dominant spaces in which users, particularly children and young people, are able to explore their identities and how they represent themselves. To participate in this space, users are nudged into making public personal information through posts and comments, as well as to divulge personal preferences and interests through 'likes' or by sharing other people's content. But social media companies are also able to gain much deeper

64. The calculation was made by two professors at Carnegie Mellon University in the USA. See Shoshana Zuboff, *The Age of Surveillance Capitalism*, 2019, pp. 48-50.
65. The HRC has referred to privacy as "a sphere of a person's life in which he or she can freely express his or her identity". See HRC, Views: *A Coeriel and M Aurik v. the Netherlands*, 9 December 1994, UN Doc. CCPR/C/92/D/453/1991, para. 10.2. Philip Agre and Marc Rotenburg (editors), *Technology and Privacy: The New Landscape,* 1998.
66. UN High Commissioner for Human Rights, *Report on Best Practices and Lessons Learned on How Protecting and Promoting Human Rights Contribute to Preventing and Countering Violent Extremism*, 21 July 2016, UN Doc. A/HRC/33/29, para. 58; Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, 23 September 2014, UN Doc. A/69/397, para. 47; OHCHR, *The Right to Privacy in the Digital Age*, 30 June 2014 (previously cited), para. 25.

insights into the private lives of platform users through data on how they engage with and how they behave on their platforms.

Data collected and aggregated to create profiles of children may be attached to those individuals for the rest of their lives. People that they follow, videos that they watch, posts that they like and choices that they make online have the potential to boomerang back on them into adulthood with potential to affect their futures in ways never experienced by previous generations. This is all the more important given that research shows that children and young people may not necessarily be fully aware of the levels of surveillance they are subjected to on social media platforms.[67]

4.2 RIGHTS TO FREEDOM OF THOUGHT AND OPINION

The right to freedom of opinion is protected by Article 19(1) of the ICCPR, which states that "[e]veryone shall have the right to hold opinions *without interference*" (emphasis added). The right to freedom of thought is protected by Article 18(1) of the ICCPR, under which "[e]veryone shall have the right to freedom of thought, conscience and religion," which includes the freedom to have or to adopt chosen beliefs and to express them, either individually or in community with others and in public or private.[68] The explicit right of children to freedom of thought is reinforced by Article 14 of the CRC.

Unlike the rights to freedom of expression and to manifest religion or belief, which can be limited by law under certain conditions,[69] the rights to freedom of thought, conscience, religion and belief and to hold opinions are absolute and unconditionally protected including under Article 18 and 19(1) of the ICCPR. In other words, the thoughts, beliefs, and opinions that a person holds inside their head can be never legitimately interfered with, even if limitations may be placed on how they are manifested or expressed.

The UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Expression (UN Special Rapporteur on freedom of expression), has highlighted the way in which new questions have been raised "about the types of coercion or inducement that may be considered an interference with the right to form an opinion" by the intersection of technology and content curation.[70] The Special Rapporteur has argued that, "at the very least", companies should "provide meaningful information about how they develop and implement criteria for curating and personalizing content on their platforms, including policies and processes for detecting social, cultural or political biases in the design and development of relevant artificial intelligence systems."[71]

Like the right to privacy, the rights to freedom of thought and freedom of opinion also comprise three elements: the right to keep your thoughts and opinions private; the right not to have your thoughts and opinions manipulated; and the right not to be penalized for your thoughts and opinions.[72] And, as with the right to privacy, the surveillance-based business model, on which TikTok and other social media platforms base their businesses, has implications for all three elements, but in particular the first element – the right to keep your thoughts and opinions private. Indeed, this business model which, as described in Chapter 3.1, "Surveillance-Based Business Model", involves the massive

67. Mariya Stoilova and others, "Digital by default: children's capacity to understand and manage online data and privacy", 3 November 2020, Media and Communication, Volume 8, Issue 4, eprints.lse.ac.uk/107114/; Kathryn Montgomery and others, "Children's privacy in the big data era: Research opportunities", 1 November 2017, Pediatrics, Volume 140, Issue Supplement 2, https://publications.aap.org/pediatrics/article/140/Supplement_2/S117/34190/Children-s-Privacy-in-the-Big-Data-Era-Research?autologincheck=redirected
68. ICCPR, Article 18.
69. These rights can be limited when necessary and proportionate, in order to achieve a legitimate aim. See ICCPR, Articles 18(3) and 19(3).
70. Report of the Special Rapporteur on freedom of expression, 29 August 2018, UN Doc. A/73/348, para. 24.
71. Report of the Special Rapporteur on freedom of expression, 29 August 2018 (previously cited), para. 26.
72. Evelyn Aswad, "Losing the Freedom to be Human", 29 February 2020, Columbia Human Rights Law Review, Volume 52, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3635701

collection of intimate personal data on all its users, often including beyond the individual platforms themselves, poses a direct threat to the right to freedom of thought and opinion in a manner and on a scale hitherto unknown.

It is generally accepted that children's capacities to understand their lives and make decisions that affect them evolve as they get older. Recognizing this, the CRC makes explicit the importance of considering the "evolving capacities of the child" in the design and implementation of measures to protect them.[73] Neuroscientists are still trying to understand how modern technology affects the brains of children and young people. However, the "heightened sensitivity to rewards" of children appears to promote both positive behaviours but also make them more likely to engage in risky behaviours.[74] Research also shows that rational thinking as opposed to emotional processing does not fully develop until the mid-twenties.[75] Teenagers are therefore much more likely than adults to act impulsively and to experience strong emotional reactions to external stimuli.[76]

The role of social media in the developmental stages of children and young people's lives, is becoming increasingly clear, as is the enormous influence exerted by them over young people's moods, perceptions and self-image through both platform design and the content they recommend.[77]

This can undermine the right not to have your thoughts and opinions manipulated because the thoughts, opinions, and indeed emotions and identities, of children and young people may be particularly influenced by the content to which they are exposed which, on social media platforms includes targeted amplified content and targeted advertisements.

4.3 THE RIGHT TO NON-DISCRIMINATION

The right to equality and non-discrimination is a fundamental principle underpinning all human rights[78] and is protected by international and regional human rights instruments, including the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD) and the ICCPR. Discrimination is defined broadly to include discrimination on the basis of race, colour, sex, language, religion, political or other opinion, descent or national or ethnic origin, birth or status.[79]

The Committee on the Elimination of Racial Discrimination, responsible for monitoring the implementation of the ICERD by states parties, has emphasized that the principle of equality must be

73. CRC, Articles 5 and 14.
74. Zara Abrams, "What neuroscience tells us about the teenage brain", 25 August 2022, Monitor on Psychology, Volume 53, Issue 5, https://www.apa.org/monitor/2022/07/feature-neuroscience-teen-brain
75. University of Rochester Medical Centre, Health Encyclopaedia, "Understanding the teen brain", 2023, https://www.urmc.rochester.edu/encyclopedia/content.aspx?contenttypeid=1&contentid=3051 (accessed on 14 September 2023).
76. BBC, "The biggest myths of the teenage brain", 7 September 2022, https://www.bbc.com/future/article/20220823-what-really-goes-on-in-teens-brains
77. Reset Australia, *Surveilling Young People Online: An Investigation into Tiktok's Data Processing Practices*, July 2021, https://au.reset.tech/uploads/resettechaustralia_policymemo_tiktok_final_online.pdf https://au.reset.tech/uploads/resettechaustralia_policymemo_tiktok_final_online.pdf; Jacopo Pruccoli and others, "The use of TikTok among children and adolescents with eating disorders: Experience in a third-level public Italian center during the SARS-CoV-2 pandemic", 30 July 2022, Italian Journal of Pediatrics, Volume 48, https://doi.org/10.1186/s13052-022-01308-4; Reset Australia, *Designing for Disorder: Instagram's Pro-Eating Disorder Bubble in Australia*, April 2022, https://au.reset.tech/uploads/insta-pro-eating-disorder-bubble-april-22-1.pdf https://au.reset.tech/uploads/insta-pro-eating-disorder-bubble-april-22-1.pdf; Tech Transparency Project, "'Thinstagram': Instagram's algorithm fuels eating disorder epidemic", 8 December 2021, https://www.techtransparencyproject.org/articles/thinstagram-instagrams-algorithm-fuels-eating-disorder-epidemic; Wall Street Journal, "Facebook knows Instagram is toxic for teen girls company documents show", 14 September 2021, https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739
78. "Non-discrimination and equality are fundamental components of international human rights law and essential to the exercise and enjoyment of economic, social and cultural rights", Committee on Economic, Social and Cultural Rights, General Comment 20: Non-discrimination in Economic, Social and Cultural Rights (Article 2, para. 2) 2 July 2009, UN Doc. E/C.12/GC/20, para. 2; "Non-discrimination, together with equality before the law and equal protection of the law without any discrimination, constitute a basic and general principle relating to the protection of human rights.", HRC, General Comment18: Non-discrimination, 10 November 1989, UN Doc. HRI/GEN/1/Rev.9 (Vol. I) (p. 195), para. 1.
79. ICERD, Article 1 and ICCPR, Article 26.

understood in the broadest sense, to include both "formal equality before the law", and "substantive or de facto equality in the enjoyment and exercise of human rights".[80]

The right of children to be protected from all forms of discrimination is expressly reiterated in Article 2 of the CRC. Furthermore, the Committee on the Rights of the Child has identified the obligation of states to ensure that all children within their jurisdiction enjoy the rights laid out in the CRC without discrimination of any kind as one of the four general principles in light of which all the rights enshrined in the CRC should be interpreted and implemented.[81]

Social media companies can undermine the right to non-discrimination through various practices, including by the way in which content and advertisements are targeted, through the amplification of content which discriminates against a particular category of persons or community, and/or through the application of policies in a discriminatory manner. For instance, social media companies risk abusing the right to non-discrimination through their ad practices and the categories that they offer in order to enable advertisers to target selected users. For example, in 2021, it was reported that Google had allowed employers and landlords to exclude people who had not specified whether they were male or female, including non-binary and trans people, from seeing their advertisements for jobs or accommodation by specifying that Google not show ads to people of "unknown gender."[82]

> **"My main concern is whether the information is being sold for targeted advertising because usually when on social media, I get offers of the things I had previously searched for on another platform... It becomes more than just coincidence."** "Lineo", 19, Lesotho, 2022

Even where advertisers do not proactively select categories of persons that they wish to target or exclude related to protected characteristics, in many cases, because those categories are not offered by social media platforms, it is possible that the algorithm that is involved in the ad delivery excludes certain people from seeing certain jobs based on age or gender, two characteristics that are protected in many countries' equality or non-discrimination legislation.

A 2021 report by EDRi showed how targeted online advertising can have discriminatory effects in a number of different ways including targeting that leads to unfair exclusion, including from housing and job ads; harmful targeting, such as when an ad seems to be based on knowledge about protected categories, which can be distressing and is an invasion of privacy; and when users are misclassified through profiling, which may result in ad targeting that is discriminatory and their missing out on opportunities.[83]

Amnesty International's research also shows how social media companies can contribute to discrimination by amplifying harmful and discriminatory content. Its report, *The Social Atrocity* found that Meta's content-shaping algorithms and reckless business practices facilitated and enabled discrimination and violence against the predominantly Muslim Rohingya community in Myanmar. Meta's algorithms proactively amplified and promoted content which incited violence, hatred, and discrimination against the Rohingya exacerbating long-standing discrimination and substantially increasing the risk of an outbreak of mass violence in the months and years leading up to atrocities in 2017.[84]

---

80. UN Committee on the Elimination of Racial Discrimination, General Recommendation 32: The Meaning and Scope of Special Measures in the International Convention on the Elimination of All Forms Racial Discrimination, 24 September 2009, UN Doc. CERD/C/GC/32, para. 6.
81. UN Committee on the Rights of the Child, General Comment 5: General Issues of Implementation of the Convention on the Rights of the Child (Articles 4, 42 and 44, para. 6), 27 November 2003, UN Doc. CRC/GC/2003/5 and General Comment 14: The Right of the Child to Have His or Her Best Interests Taken as a Primary Consideration (Article 3, para. 1),29 May 2013, UN Doc. CRC /C/GC/14.
82. The Markup, "Google Has Been Allowing Advertisers to Exclude Nonbinary People from Seeing Job Ads", 11 February 2021, https://themarkup.org/google-the-giant/2021/02/11/google-has-been-allowing-advertisers-to-exclude-nonbinary-people-from-seeing-job-ads. Google subsequently committed to update its policies and enforcement to restrict advertisers from either targeting or excluding users on the basis of the "gender unknown" category.
83. European Digital Rights (EDRi), *How online ads discriminate,* 16 June 2021, https://edri.org/our-work/how-online-ads-discriminate/
84. Amnesty International, *Myanmar: The Social Atrocity* (previously cited).

Amnesty International's 2023 report *'A death sentence for my father': Meta's contribution to human rights abuses in northern Ethiopia* ('*A death sentence for my father*) exposes how many of the same systemic failures that occurred in the context of Myanmar were repeated in Ethiopia. Viral Facebook posts containing dehumanizing narratives, including messages advocating hatred that incited violence, hostility and discrimination against the Tigrayan community, were a dominant feature of the targeting of the community during the armed conflict. Amnesty International found that Meta contributed to the negative human rights impacts suffered by the Tigrayan community, as a result of the role that the platform features – which constitute the foundation of its business model (particularly algorithmic amplification and correspondingly, virality) – played in actively amplifying content which advocated hatred constituting incitement to violence, hostility and discrimination against the Tigrayan community.[85]

Amnesty International's briefing *Digitally Divided: Technology, Inequality and Human Rights* has also shown how... content moderation is an important yet largely hidden component of many social media companies' business models, in which content that violates a platform's terms of service is identified, flagged, investigated, and deleted, shielding users from viewing violent, dangerous, or abusive content, and protecting the company from legal liability when such content violates local laws. Repeated investigations have shown that content moderation is mentally and emotionally difficult work, which risks causing long-term mental health effects for workers, while contractors often face unfairly low wages, exploitative working conditions, and retribution in response to organizing efforts. The systemic exploitation of workers in service of creating profit for and legally shielding such corporations demonstrates how an essential component underpinning today's online environment creates, exacerbates, and encourages multiple and intersecting inequalities across the world.[86]

4.4 MEASURES TO PROTECT THE RIGHTS AND BEST INTERESTS OF CHILDREN

PROTECTING THE BEST INTERESTS OF THE CHILD

Under international law, children are full human rights holders, independently from parents or guardians, and are also entitled to special protection, in particular under the CRC, the most widely ratified human rights treaty.[87] The CRC sets out a wide range of human rights applicable to all children and requires that the best interests of the child should be a primary consideration in all actions concerning them whether undertaken in the public or private sphere.[88] The Committee on the Rights of the Child, the body responsible for monitoring the implementation of the CRC, has described the principle of the best interests of the child as being "aimed at ensuring both the full and effective enjoyment of all the rights recognized in the Convention and the holistic development of the child".[89] The Committee has further clarified that states parties have an obligation to ensure that the private sector abides by the best interests principle when providing services to, or making decisions that affect, children.[90]

85. Amnesty International, '*A death sentence for my father*' (previously cited)
86. Amnesty International, *Digitally Divided: Technology, Inequality and Human Rights* (Index: POL 40/7108/2023), 2 October 2023, https://amnestyusa.org/wp-content/uploads/2023/09/Amnesty-Tech-and-Inequality-Report-Digitally-Divided.pdf
87. The US is a notable non-ratifier of the CRC.
88. CRC, Article 3(1).
89. UN Committee on the Rights of the Child, General Comment 14: The right of the child to have his or her best interests taken as a primary consideration (Article 3, para. 1), 29 May 2013, UN Doc. CRC /C/GC/14, para. 4.
90. UN Committee on the Rights of the Child, General Comment 14 (previously cited), para. 14(c).

In its 2021 General Comment 25 on children's rights in the digital environment, the Committee stressed that 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."[91] It further called on states to ensure that "digital service providers offer services that are appropriate for children's evolving capacities."[92]

PROTECTING CHILDREN'S RIGHTS TO PRIVACY, THOUGHT AND OPINION

As noted above, the CRC includes protections for children's right to privacy and the Committee on the Rights of the Child has set out measures that should be taken by states to ensure that companies prevent their networks and online services from being used in ways that threaten children's rights, including their rights to privacy, and to provide remedies for violations and abuses.[93]

To this end, the Committee has recommended a series of measures to be taken by states parties including:

- Adopt laws that "include strong safeguards, transparency, independent oversight and access to remedy," and require "the integration of privacy-by-design into digital products and services that affect children";[94]
- Institute regular reviews of privacy and data protection legislation and ensure that procedures and practices prevent deliberate infringements or accidental breaches of children's privacy";[95]
- Where consent is sought to process children's data, states parties should ensure that measures are in place to obtain meaningful and informed consent from either the child or their parent or caregiver prior to processing the data.[96]
- Institute a requirement on companies to conduct child rights due diligence – including carrying out child rights impact assessments and disclosing these to the public – which takes into consideration the different, and sometimes more severe, impacts of technology, online services, and the digital environment on children;[97]
- Require all businesses that affect children's rights in relation to the digital environment to implement codes of practice, transparency, and accountability to achieve the highest standards of ethics, privacy, and safety in relation to their impact on children. This includes "the provision of age-appropriate explanations to children, or to parents and caregivers of very young children, of their terms of service";[98]
- Put in place processes to prevent, monitor, investigate and punish abuses of children's rights by businesses.[99] Since it can be difficult for children to seek remedy for abuses by business enterprises[100] particularly where they are not located in the country of residence of the affected child, the Committee has recommended that states should consider their obligations under the CRC in the global context of companies' extraterritorial and transnational activities and ensure that oversight agencies "investigate complaints and provide adequate remedies for violations or abuses of children's rights in the digital environment."[101]

91. UN Committee on the Rights of the Child, General Comment 25: Children's Rights in Relation to the Digital Environment, 2 March 2021, UN Doc. CRC/C/GC/25, para. 12.
92. UN Committee on the Rights of the Child, General Comment 25 (previously cited), para. 20.
93. UN Committee on the Rights of the Child, General Comment 25 (previously cited), para. 36.
94. UN Committee on the Rights of the Child, General Comment 25 (previously cited), para. 70.
95. UN Committee on the Rights of the Child, General Comment 25 (previously cited), para. 70.
96. UN Committee on the Rights of the Child, General Comment 25 (previously cited), para. 71.
97. UN Committee on the Rights of the Child, General Comment 16: State Obligations Regarding the Impact of The Business Sector on Children's Rights, 17 April 2013, UN Doc. CRC/C/GC/16, paras. 50 & 62-65.
98. UN Committee on the Rights of the Child, General Comment 25 (previously cited), para. 39.
99. UN Committee on the Rights of the Child, General Comment 25 (previously cited), para. 38.
100. UN Committee on the Rights of the Child, General Comment 16 (previously cited), paras 66-67.
101. UN Committee on the Rights of the Child, General Comment 16 (previously cited), paras 30 & 43.

The Committee has also issued specific guidance to prevent interference with children's freedom of thought and belief in the digital environment and recommended that states ensure that "automated systems or information filtering systems are not used to affect or influence children's behaviour or emotions or to limit their opportunities or development."[102]

As noted above, data collecting and processing by social media platforms may constitute arbitrary or unlawful interference with children's right to privacy,[103] and the Committee on the Rights of the Child has underscored that any interference with the privacy of children is only permissible if it meets the three-part test of being legitimate, necessary, and proportionate.[104]

It has also emphasised the importance of education to help children understand the digital environment (including its infrastructure, business practices, persuasive strategies and the uses of automated processing and personal data and surveillance, and of the possible negative effects of digitalization on societies),[105] and to enable them to make fully informed choices about their engagement with it. To this end, the Committee has recommended that states parties develop comprehensive digital literacy curricula to be taught from pre-school and throughout all subsequent levels of schooling, to give children the knowledge and skills to safely engage with and navigate the digital environment.[106]

PROTECTING CHILDREN IN THE CONTEXT OF CORPORATE ACTIVITY

The Committee on the Rights of the Child has also set out measures (in addition to those on due diligence above) required of states to protect children's human rights in the context of corporate activities. These measures include adopting laws, regulations and policies to protect children's rights and best interests and monitoring their enforcement as well as investigating, adjudicating and ensuring redress for abuses of children's rights caused or contributed to by a business enterprise. States are considered "responsible for infringements of children's rights caused or contributed to by business enterprises where it has failed to undertake necessary, appropriate, and reasonable measures to prevent and remedy such infringements or otherwise collaborated with or tolerated the infringements."[107]

The Committee has also set out specific guidance concerning marketing and advertising, which is relevant to the surveillance-based business model and its use of targeted advertising, because of the powerful influence of such marketing and advertisements on children's self-image, and the risk that children will uncritically consume and use products that may be harmful to them. To this end the Committee has called on states to "ensure that marketing and advertising do not have adverse impacts on children's rights by adopting appropriate regulation and encouraging business enterprises to adhere to codes of conduct and use clear and accurate product labelling and information that allow parents and children to make informed consumer decisions."[108]

The Committee has also highlighted that "States are required to prevent discrimination in the private sphere in general and provide remedy if it occurs."[109]

PROTECTING CHILDREN FROM TARGETTED ADVERTISING

The Committee on the Rights of the Child has stressed that states should "ensure that businesses do not target children using... techniques designed to prioritize commercial interests over those of the child."[110]

---

102. UN Committee on the Rights of the Child, General Comment 25 (previously cited), para. 62.
103. UN Committee on the Rights of the Child, General Comment 25 (previously cited), para. 68.
104. UN Committee on the Rights of the Child, General Comment 25 (previously cited), para. 69.
105. UN Committee on the Rights of the Child, General Comment 25 (previously cited), para. 105.
106. UN Committee on the Rights of the Child, General Comment 25 (previously cited), para. 104.
107. Committee on the Rights of the Child, General Comment No. 16, 17 April 2013, UN Doc. CRC/C/GC/16, para. 28.
108. UN Committee on the Rights of the Child, General Comment 16 (previously cited), para. 59.
109. UN Committee on the Rights of the Child, General Comment 16 (previously cited), para. 14.
110. UN Committee on the Rights of the Child, General Comment 25 (previously cited), para. 110.

In its General Comment 25, it notes that both the processing of personal data and targeted advertising can intentionally and unintentionally violate children's rights by their design, including through "advertising design features that anticipate and guide a child's actions towards more extreme content, automated notifications that can interrupt sleep or the use of a child's personal information or location to target potentially harmful commercially driven content."[111]

The Committee has stressed that the states parties to the CRC "should make the best interests of the child a primary consideration when regulating advertising and marketing addressed to and accessible to children."[112] It has also advised that "sponsorship, product placement and all other forms of commercially driven content should be clearly distinguished from all other content and should not perpetuate gender or racial stereotypes."[113]

Importantly the Committee has explicitly called upon states to prohibit by "law the profiling or targeting of children of any age for commercial purposes on the basis of a digital record of their actual or inferred characteristics, including group or collective data, targeting by association or affinity profiling."[114] It has additionally called for a ban on "practices that rely on neuromarketing, emotional analytics, immersive advertising and advertising in virtual and augmented reality environments to promote products, applications and services from directly or indirectly engaging with children."[115]

Given that the surveillance-based business model of social media involves an abuse of the rights to privacy and freedom of thought and poses risks to a range of other rights, including the right to non-discrimination, it is clear that this extractive business model and its data practices cannot be in the best interests of the child.

> **"I'm scared that social media companies can use my personal information in various ways. In the grand scheme of things, I'm afraid that their usage of my personal data can contribute to the increasingly polarized political sphere.**
>
> **I acknowledge that terms of service need to be very specific thus lengthy, but I sometimes think that the writers purposely make them unreadable for the general user."**
>
> 20, "Gabriel", Philippines, 2022

111. UN Committee on the Rights of the Child, General Comment 25 (previously cited), para. 40.
112. UN Committee on the Rights of the Child, General Comment 25 (previously cited), para. 41.
113. UN Committee on the Rights of the Child, General Comment 25 (previously cited), para. 41.
114. UN Committee on the Rights of the Child, General Comment 25 (previously cited), para. 42.
115. UN Committee on the Rights of the Child, General Comment 25 (previously cited), para. 42.

5. BUSINESS AND HUMAN RIGHTS FRAMEWORK

Companies have a responsibility to respect all human rights wherever they operate in the world and throughout their operations. These widely recognized standards of expected conduct are set out in international business and human rights standards including the UN Guiding Principles on Business and Human Rights (UN Guiding Principles), and the Organisation for Economic Co-operation and Development (OECD) Guidelines for Multinational Enterprises (OECD Guidelines).[116]

This corporate responsibility to respect human rights requires companies to avoid causing or contributing to human rights abuses and address the impacts of their own business activities, or those of their business relationships in which they are involved, including by remediating any actual abuses. It also requires companies to prevent or mitigate actual and potential adverse human rights impacts directly linked to their operations, products services, through their business relationships and other entities in their value and supply chains, even if they have not contributed to the harms.[117]

The UN Guiding Principles establish that, to meet their corporate human rights responsibilities, companies should have in place ongoing and proactive human rights due diligence processes to identify, prevent, mitigate, and account for how they address their impacts on human rights. If, as part of its due diligence, a company identifies that it may cause, or has caused or contributed to, a human rights abuse, it must take measures to cease or prevent the adverse human rights impacts.

Where impacts are outside of the company's control but are nevertheless directly linked to their operations, products, or services through their relationships with other businesses or entities, the UN Guiding Principles require the company to seek to mitigate the human rights impact by exercising or seeking to improve leverage over the concerned entity or, failing this, consider ending the relationship.[118]

The OECD has provided practical guidance for conducting due diligence in its Due Diligence Guidance for Responsible Business Conduct (OECD Due Diligence Guidance).[119] This guidance, which elaborates on the due diligence responsibilities of companies under the OECD Guidelines, is designed to help companies in all sectors, regardless of size, geographic location, or value chain position, to understand

116. *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, 2011*, endorsed by the UN Human Rights Council (UNHRC), UNHRC Resolution 17/4: *Human rights and Transnational Corporations and other Business Enterprises*, adopted on 16 June 2011, UN Doc. A/HRC/RES/17/4; and OECD Guidelines for Multinational Enterprises, 2011, https://mneguidelines.oecd.org/mneguidelines. In accordance with the UN Guiding Principles, corporate responsibility to respect human rights is independent of a State's human rights obligations and exists over and above compliance with national laws and regulations protecting human rights. See UN Guiding Principles, Principle 11 and Commentary.
117. UN Guiding Principles (previously cited), Principles 11 & 13 and Commentary.
118. UN Guiding Principles (previously cited), Principle 19 and Commentary.
119. OECD, Due Diligence Guidance for Responsible Business Conduct, 2018, https://mneguidelines.oecd.org//OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf

and implement their due diligence responsibilities. The six-step framework provides detailed guidance to companies on how to:

1. Embed responsible business conduct into policies and management systems;
2. Identify and assess adverse impacts in operations, supply chains and business relationships;
3. Cease, prevent or mitigate adverse impacts;
4. Track implementation and results;
5. Communicate how impacts are addressed; and
6. Provide for or cooperate in remediation, when appropriate.

The UN Guiding Principles also require states to "protect against human rights abuse within their territory and/or jurisdiction by third parties, including business enterprises," and to take effective measures to prevent, investigate, punish and provide redress such abuse through effective policies, legislation, regulations and adjudication."[120] Furthermore, in 2017, the UN Committee on Economic, Social and Cultural Rights confirmed that: "The extraterritorial obligation to protect requires States parties to take steps to prevent and redress infringements of Covenant rights that occur outside their territories due to the activities of business entities over which they can exercise control, especially in cases where the remedies available to victims before the domestic courts of the State where the harm occurs are unavailable or ineffective."[121]

An important element of due diligence is transparency and publicly accounting for how a company has identified, prevented, or mitigated potential or actual adverse impacts on human rights. As the UN Guiding Principles make clear, companies "need to know and show that they respect human rights".[122] In this case, "showing involves communication, providing a measure of transparency and accountability to individuals or groups who may be impacted and to other relevant stakeholders."[123] The Committee on the Rights of the Child has likewise emphasized that states should encourage – and where appropriate, require – companies to publish details of what measures they have taken to address impacts on children's human rights caused by their activities.[124]

As affirmed by Office of the High Commissioner for Human Right's (OHCHR) B-Tech project, in the technology sector the corporate responsibility to respect human rights, which includes the responsibility to conduct human rights due diligence, implies that companies should: i) pro-actively identify when their business model-driven practices, and related technology designs, create or exacerbate human rights risks; and ii) take action to address these situations – whether by mitigating risks within existing business models or by innovating entirely new ones.[125]

120. UN Guiding Principles (previously cited), Principle 1.
121. UN Committee on Economic, Social (CESCR), General comment No. 24 (2017) on State obligations under the International Covenant on Economic, Social and Cultural Rights in the context of business activities (UN Doc. E/C.12/GC/24), 2017, para. 30., https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-24-2017-state-obligations-context
122. UN Guiding Principles (previously cited), Commentary to Principle 15.
123. UN Guiding Principles (previously cited), Commentary to Principle 21.
124. Committee on the Rights of the Child, General Comment No. 16 (previously cited), para. 65.
125. OHCHR, *Addressing Business Model Related Human Rights Risks: A B-Tech Foundational Paper*, July 2020, https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/B_Tech_Foundational_Paper.pdf

6. EFFORTS AROUND THE WORLD TO REGULATE

With technology developing at an ever-faster pace, lawmakers and regulatory efforts around the world are struggling to keep up. There has been little progress towards addressing the systemic risks associated with large social media platforms, and to date few states or regional organizations have adopted legislation.

According to the UN Conference on Trade and Development, in 2021 137 out of 194 countries (71%) had put in place data protection and privacy legislation. Africa and Asia had below average numbers of countries of adoption of such legislation with 61 and 57 per cent of countries respectively having adopted such legislations. The share in the least developed countries is only 48 per cent.[126]

Among the few jurisdictions that have taken action is the European Union (EU), whose Digital Service Act (DSA), adopted in July 2022, became the first major regional level "Big Tech" regulation, aimed at limiting the harmful effects of social media platforms, including by banning intrusive "targeted advertising" towards children.[127] The DSA imposes obligations on the largest online platforms, including TikTok, to assess their systemic risks, including risks to public health and children, to take measures to mitigate these risks and to subject themselves to independent audits to assess their compliance with these obligations (albeit with many questions remaining concerning the precise nature and enforcement of these measures).[128] Under the DSA, TikTok and other very large platforms are also required to provide users with at least one feed which is not based on user profiling. Amnesty International has described this opt-in approach a "missed opportunity" because changing settings to more privacy-respecting options is often cumbersome and users tend to stick to the default setting.[129]

The effectiveness of the DSA is yet to be tested; some of the obligations on very large online platforms such as the submission of risk assessments took effect in August 2023, but the DSA does not fully enter into force until 2024. While the DSA seeks to curtail certain risks associated with the surveillance-based business model of social media companies, for example by banning targeted advertising towards children, it does not ban the business model as a whole and is thus limited. Nonetheless, the DSA

126. UN Conference on Trade and Development, Data Protection and Privacy Legislation Worldwide, https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (accessed 17 October 2023)
127. EU, Regulation 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2022%3A277%3ATOC&uri=uriserv%3AOJ.L_.2022.277.01.0001.01.ENG
128. For a detailed analysis of the DSA see Amnesty International, *What the EU's Digital Services Act Means for Human Rights and Harmful Big Tech Business Models*, (Index: POL 30/5830/2022), 7 July 2022, https://www.amnesty.org/en/documents/pol30/5830/2022/en; Euractiv, "Europe enters patchy road to audit online platforms' algorithms", 7 July 2023, https://www.euractiv.com/section/platforms/news/europe-enters-patchy-road-to-audit-online-platforms-algorithms/
129. Alfred Ng, "Default settings for privacy – we need to talk", 21 December 2019, https://www.cnet.com/tech/tech-industry/default-settings-for-privacy-we-need-to-talk/

represents the most ambitious piece of platform regulation to date. Even though the DSA is limited in scope and application to platforms' operations in the EU, it nonetheless raises hopes of positive ripple effects beyond the EU as changes implemented inside the EU might be more easily extended or copied over into legislative proposals elsewhere.

In the UK, the Online Safety Bill, passed in September 2023, imposes new obligations on platforms with the intention of creating a safer online environment, with special protections applied to under 18s.[130] The Online Safety Bill was drafted to add to the privacy protections and data minimization requirements contained in the UK Children's Code, which first imposed a duty on online services to only engage in the "profiling" of children if they have "appropriate measures in place to protect the child from any harmful effects (in particular, being fed content that is detrimental to their health or well-being)".[131]

New regulations in the USA remain deadlocked at the federal level.[132] However, several states have passed laws regulating online spaces. Among these is California whose Age-Appropriate Design Code Act will require platforms that "are likely to be accessed by children" to offer children a greater level of privacy through their default settings and prohibit the use of a child's information "in a way that the business knows, or has reason to know, is materially detrimental to the physical health, mental health, or well-being of a child".[133] The Act was however blocked by a federal judge in September 2023 while a lawsuit lodged by a tech industry group proceeds, which argues that the law violates the First Amendment.[134] Similar to the DSA, companies will have to conduct a non-public data protection impact assessment to identify whether a platform's design elements or algorithms could harm children. Although many child rights advocates have welcomed the Act as a step towards a safer online space,[135] privacy and free speech advocates have raised privacy concerns about the possible negative implications of a wider use of age verification measures.[136]

In the meantime, several US states have adopted legislation giving parents unprecedented access to and control over their children's social media accounts, raising concerns about children's privacy.[137]

While the introduction of a ban on targeted advertising to children under 18 in Europe is a step in the right direction and will create more privacy-respecting experiences for teen users, research has found that "the best way to keep children safe from the sale of their personal data on the internet is to ban all online advertising which targets users based on personal data".[138] Governments around the

130. UK Department for Digital, Culture, Media and Sport, Online Safety Bill (as amended in Committee), https://bills.parliament.uk/bills/3137
131. Information Commissioner's Office (ICO), Age-appropriate design code, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/code-standards/ (accessed on 13 July 2023).
132. Of the multiple proposed federal-level bills relating to platform regulation, only the Kids Online Safety Act (KOSA) looks likely to be passed in the near term. KOSA combines elements of the California Design Code and the EU's DSA, requiring any large platform likely to be accessed by under-17s to publish reports on compliance activities, to implement "measures in its design and operation of products and services to prevent and mitigate" harms and to offer young users ways to opt-out of personalized recommendation-based feeds. See Congress.gov, Text - S.1409 - 118th Congress (2023-2024): Kids Online Safety Act, 2 May 2023, https://www.congress.gov/bill/118th-congress/senate-bill/1409/text
133. Alexander Misakian and Tiffany Young, "California enacts the California Age-Appropriate Design Code Act", 20 September 2022, https://www.foley.com/en/insights/publications/2022/09/california-enacts-age-appropriate-design-code-act
134. The Verge, "Court blocks California's online child safety law", 18 September 2023, https://www.theverge.com/2023/9/18/23879489/california-age-appropriate-design-code-act-blocked-unconstitutional-first-amendment-injunction
135. See for example: Fairplay, "Josh Golin statement regarding California Age Appropriate Design Code", 23 May 2022, https://fairplayforkids.org/josh-golin-ca-aadc/
136. Iapp, "California Age Appropriate Design Code final passage brings mixed reviews", 31 August 2022, https://iapp.org/news/a/california-age-appropriate-design-code-final-passage-brings-mixed-reviews/
137. NPR, "Utah's new social media law means children will need approval from parents", 24 March 2023, https://www.npr.org/2023/03/24/1165764450/utahs-new-social-media-law-means-children-will-need-approval-from-parents; CNN, "Arkansas governor signs sweeping bill imposing a minimum age limit for social media usage", 12 April 2023, https://edition.cnn.com/2023/04/12/tech/arkansas-social-media-age-limit/index.html; CNN, "Louisiana lawmakers approve parental consent bill for kids' social media use and other online services", 8 June 2023, https://edition.cnn.com/2023/06/08/tech/louisiana-parental-consent-bill-social-media/index.html
138. New Economics Foundation, *Ban Surveillance Advertising To Protect Kids Online*, May 2021 neweconomics.org/2021/05/ban-surveillance-advertising-to-protect-kids-online

world need to urgently make further and faster progress towards protecting people from the systemic risks related to social media companies' business model by taking effective measures to prevent, investigate, punish, and provide redress for abuses through effective policies, legislation, regulations and adjudication.

6.1 SANCTIONS AGAINST TIKTOK FOR VIOLATING DATA PROTECTION/PRIVACY LAWS

There is growing awareness of the risks posed by social media to the right to privacy, and the particular implications that this has for children. Mounting public concern and pressure has resulted in an increasing number of investigations into the misuse of data, including that of children.

TikTok is not alone in being found to be in violation of data protection regulations and sanctioned. For example, on 17 July 2023, Norway's Data Protection Authority temporarily banned Meta's online platforms, including Facebook and Instagram, from tracking users online to target them with advertising without their consent.[139] This followed a ruling by the Court of Justice of the European Union (CJEU) earlier the same month on a case brought by the German antitrust watchdog, the Federal Cartel Office, which ordered Meta to stop combining user data across its family of social platforms (Facebook, Instagram, Messenger and WhatsApp) without their consent. The ruling also found that consent is the only appropriate and adequate legal basis for the system of personalized content and targeted advertising, based on profiling and behavioural predictions, that Meta uses and which forms its primary revenue-generating activity.[140] This ruling was important because it established that Meta could not bypass the consent requirement within the GDPR for tracking and online ads by relying on other legal bases for processing data and arguing that ads are a part of the "service" that it contractually owes the users.

TikTok has not been immune to this sort of regulatory action and there have been a number of important cases concerning its privacy and data collection policies and practices relating to children.

In 2019, the US Federal Trade Commission (FTC) fined Musical.ly, which by then had been acquired by ByteDance and absorbed into TikTok (see Chapter 3.2 "What is TikTok"), US$5.7 million for illegally collecting data, including the names, email addresses, pictures, and locations, of children under the age of 13. This record fine for violations of American children's privacy was part of a settlement between the FTC and TikTok although, according to TikTok, the illegal data collection predated its 2018 merger with Musical.ly and its practices had since changed.[141]

In its filing, the FTC noted that many TikTok users list their ages in their bios on their profiles meaning the app had "actual knowledge" that they were under 13 but was still illegally collecting their data without parental consent. The FTC said that it had received thousands of complaints from parents of young children using the app.

---

139. Amnesty International, "Norway: Temporarily banning Meta's invasive advertising is a welcome step for privacy rights", 17 July 2023, https://www.amnesty.org/en/latest news/2023/07/norway-temporarily-banning-metas-invasive-advertising-is-a-welcome-step-for-privacy-rights/. Daily fines were also imposed, starting from August 2023, for non-compliance with the order's requirement that Meta could show customized ads but only based on information given by users in the "about" section of their profiles. See, Guardian, "Norway to fine Meta $98,500 a day over user privacy breach from 14 August", 8 August 2023, https://www.theguardian.com/technology/2023/aug/07/norway-meta-fine-user-privacy-breach-targeted-ads; TechCrunch, "Meta denied injunction against Norway's ban order on its surveillance ads", 6 September 2023, https://techcrunch.com/2023/09/06/meta-surveillance-ads-injunction-fail/
140. noyb, "CJEU declares Meta/Facebook's GDPR approach largely illegal", https://noyb.eu/en/cjeu-declares-metafacebooks-gdpr-approach-largely-illegal
141. FTC, "Video social networking app musical.ly agrees to settle FTC allegations that it violated children's privacy law", 27 February 2019, https://www.ftc.gov/news-events/news/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc-allegations-it-violated-childrens-privacy

TikTok responded to the fine by announcing that it would require new users, and prompt existing users, to verify their age. The social media app also launched "TikTok for Younger Users", which allows under 13s, although only in the USA, to set up an account through which they can access a limited "age-appropriate" app experience. "TikTok for Younger Users", also includes additional safety and privacy protections for under 13-year-olds in order to comply with US regulations on children's privacy.[142] The company also agreed to delete the data it had collected on children.[143]

In July 2021, the Dutch Data Protection Authority (Dutch DPA) fined TikTok €750,000 (US$882,975)[144] for violating the privacy of young children. The DPA found that, because information relating to privacy provided to Dutch users, including children, when installing and using the app was only available in English, TikTok had failed to provide an adequate explanation of how the app collects, processes, and uses personal data. As such, TikTok had violated privacy legislation, which is predicated on the idea that people must be given a clear, understandable explanation of what is being done with their personal data.[145]

In April 2023, the UK Information Commissioner's Office (ICO) fined TikTok £12.7 million (US$ 15,877,540),[146] for breaches of the UK's data protection laws, representing one of the biggest fines that it has issued to date. According to the ICO, in 2020 TikTok allowed up to 1.4 million children in the UK under the age of 13 to use its platform, in breach of its own rules under which an individual must be 13 or older to create an account. It found that TikTok was in violation of UK data protection law, that requires organizations that collect and use personal data when offering "information society services" to children under the age of 13 to have the consent of their parents or guardians. The ICO concluded that, not only had TikTok failed to obtain parental or carer consent but had also "failed to carry out adequate checks to identify and remove underage children from its platform." It additionally found that TikTok had failed "to provide proper information to people using the platform about how their data is collected, used, and shared in a way that is easy to understand" and "to ensure that the personal data belonging to its UK users was processed lawfully, fairly and in a transparent manner."[147]

In September 2023, the Irish Data Protection Commission (DPC) fined TikTok €345 million (US$368.1 million)[148] for breaches of EU's General Data Protection Regulation (GDPR) regarding its handling of children's data. Among the breaches were making child users' accounts public by default (the DPC found that users aged between 13 and 17 were guided through the sign-up process in a way that resulted in their accounts being set to public by default with the result that anyone could see content or comments on it), failing to give transparent information to child users, allowing an adult accessing a child's account through the "family pairing" setting to enable direct messaging for over-16s, and not properly taking into account the risks posed to children under-13 on the platform whose accounts were made public by default. It also found that the "family pairing" tool, which gives an adult control over a child's account settings, did not verify whether the "paired" adult was a parent or guardian of the child user.[149]

The ruling related to problems with TikTok's privacy policy that was in place between 31 July and 31 December 2020 which TikTok say it has since addressed. It has also adjusted settings on the app so that, since 2021 all existing and new TikTok accounts for 13- to 15-year-olds are set to private by default.

The following chapter will provide an analysis of TikTok's most up-to-date privacy policies.

---

142. TikTok Newsroom, "TikTok for Younger users", 13 December 2019, https://www.ftc.gov/news-events/news/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc-allegations-it-violated-childrens-privacy
143. The Verge, "TikTok users over 13 are having their accounts deleted after putting in the wrong birthdays", 28 February 2019, https://www.theverge.com/2019/2/28/18245011/tiktok-age-coppa-child-privacy-accounts-deleted-ftc-requirement
144. Calculation based on an exchange rate of 1 Euro to 1.1773 US dollars, on 22 July 2021, Exchange Rates currency convertor.
145. European Data Protection Board, "Dutch DPA: TikTok fined for violating children's privacy", 22 July 2021, https://edpb.europa.eu/news/national-news/2021/dutch-dpa-tiktok-fined-violating-childrens-privacy_en
146. Calculation based on an exchange rate of 1 British pound to 1.2503 US dollars on 4 April 2023, Exchange Rates currency convertor.
147. ICO, "ICO fines TikTok £12.7 million for misusing children's data", 4 April 2023, https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/04/ico-fines-tiktok-127-million-for-misusing-children-s-data/
148. Calculation based on an exchange rate of 1 Euro to 1,067 US dollars on 15 September [2023?], Exchange Rates currency convertor.
149. Data Protection Commission, "Irish Data Protection Commission announces €345 million fine of TikTok", 15 September 2023, https://www.dataprotection.ie/en/news-media/press-releases/DPC-announces-345-million-euro-fine-of-TikTok

7. TIKTOK'S POLICIES

> ***"I think they are taken [sic] lots of data from me and I do not know in which place they are using it. Generally terms and conditions are so long to read, also as long as they want your data somehow they are stealing it from you anyway."***
>
> 23, "Nilüfer", Turkey

The following chapter reviews TikTok's three regional privacy policies, other relevant policies and publicly available information from TikTok, as well as responses received by Amnesty International from TikTok on 12 July 2023 and 29 October 2023 to questions related to the collection, storage and processing of children's data (See Chapter 1 "Methodology"). This chapter also provides analysis of how these policies contribute to the human rights abuses outlined in Chapter 4 above. It is followed by an analysis of the company's due diligence practices and the measures taken by TikTok to strengthen protections for children on the platform. This chapter will show that TikTok's business model is fundamentally incompatible with children's human rights. To the extent they have reined in any of their abusive practices and addressed concerns related to children's privacy, it has been in response to regulation in the European Economic Area (EEA)/UK/Swiss area, notably the Digital Services Act. However, even in this region, many aspects of the business model remain the same and thus an abuse of children's human rights. Furthermore, the fact that they have failed to implement these same changes globally is discriminatory against children in countries of the Global Majority.

7.1 TIKTOK'S PRIVACY POLICIES

TikTok's privacy policy is divided into three regions: EEA/UK/Switzerland,[150] United States[151] and Other Regions.[152] The three policies are broadly similar but have several important differences which means that the level of protection to children's privacy differs depending on the region in which they live. A

150. The EEA includes EU countries and also Iceland, Liechtenstein and Norway. EU countries are: Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden. TikTok, Privacy Policy (EEA/UK/Switzerland) (updated 4 May 2023), https://www.tiktok.com/legal/page/eea/privacy-policy/en
151. TikTok, Privacy Policy (United States) (updated 22 May 2023), ne https://www.tiktok.com/legal/page/us/privacy-policy/en
152. According to TikTok, the app is currently available in over 150 countries or markets. TikTok, Creator Marketplace, https://creatormarketplace.tiktok.com/ (accessed 23 October 2023). The Other Regions policy applies to all other countries outside of those that are covered by the EEA/UK/Switzerland and US policies and includes supplemental terms that are jurisdiction specific. TikTok, Privacy Policy (Other Regions), https://www.tiktok.com/legal/page/row/privacy-policy/en (updated on 4 August 2023).

table reproducing the key points from each policy can be found in Annex I, while the following provides a summary of key features and differences and an analysis of them.

To join TikTok, you must be at least 13 years old in most parts of the world, though in some countries the age is higher. This means that TikTok largely collects and processes the data of children under the age of 18 in the same way as it does for adults' data, though some greater privacy-respecting policies have been introduced for 13–17-year-olds in some parts of the world (discussed in this chapter).

Overall, there is a degree of ambiguity with respect to the types of personal data collected by TikTok, how the information collected is used and the policies do not provide sufficient detail to fully understand exactly how information is being shared or with whom. TikTok policies fail to specify the purposes of the collection of personal data in a manner that respects the principles of data protection, thereby making it impossible to assess whether the purpose is legitimate, necessary, and proportionate.

THE INFORMATION THAT TIKTOK COLLECTS

Under TikTok's three regional privacy policies, information that is provided by and collected from users is largely the same. When a user signs up to TikTok its policies state that it will collect profile information, such as name, age, username, password, language, email, phone number, social media account information, and profile image. Once a user's account is open, TikTok collects content created or published by users on the platform, including;

- Photographs, videos, audio recordings, livestreams, comments, hashtags, feedback, reviews, and associated metadata (such as when, where, and by whom the content was created).
- Features about the videos, images, and audio recordings that are part of a user's content, for example, by identifying objects and scenery, the existence or location within an image of a face or other body parts; and the text of words spoken in a user's content. TikTok states in its policies that it does this for content moderation and to provide special effects (such as video filters and avatars) and captions.
- If a user wants to connect with friends and contacts on TikTok that they are connected with on other social media platforms, TikTok will collect a user's public profile information from the other platform as well as the names and public profiles of their social network contacts.
- If a user chooses to sync their contacts, TikTok will collect information from their device's phone book such as names, phone numbers, and email addresses, and match that information to other platform users.

Amnesty International researchers conducting research on the TikTok platform for the report *Driven into Darkness* noticed that the nudging to sync contacts occurs very frequently, almost every time you open the app.

In addition, TikTok also automatically collects huge amounts of data about how users engage with the platform including information about the content they view, the duration and frequency of use, their engagement with other users, their search history and their settings. However, it is not clear for any of the three regional privacy policies whether the list of information collected under this particular category is exhaustive.

The device or technical information that TikTok collects includes the user's device model, operating system, keystroke patterns or rhythms, IP address, time zone settings, battery states and system language.

In 2022, research by a software engineer showed how TikTok tracks every tap of your screen and keyboard input (including passwords, credit card information etc.) when you open a website link and

interact with it through TikTok's in-app browser on the TikTok iOS app. Importantly, because TikTok does not offer users the option to open third party websites in the default browser on their device, if a user wants to visit a website that is linked in the app, they cannot leave the app and view it in an external browser.[153]

The researcher recognized that the findings did not necessarily mean the app is doing anything malicious, but that it is not possible to know fully what kind of data each in-app browser collects and how or if the data is being transferred or used. In response, TikTok said the research conclusions were false and misleading and that the data was collected for the sole purpose of "debugging, troubleshooting, and performance monitoring."[154]

In June 2023, TikTok released more information related to this issue, stating that the platform collects "certain keystroke patterns or rhythms for security and performance related purposes, such as to verify the authenticity of an account, for risk control, debugging, troubleshooting, and monitoring for proper performance."[155] However, it reiterated and expanded upon previous denials that it tracks key or click events, stating that:

"Prior to September 2022, when people used TikTok's in-app browser to browse a third party website, TikTok did not track which keys were pressed, only the fact that a key was pressed (a "key event") on a third-party website. Similarly, TikTok did not track which buttons were clicked on a third-party website, only the fact that a click had occurred (a "click event"), except in limited error scenarios. Moreover, starting in September 2022 for users using a current version of the App, no key events or click events were logged except when the IAB [in-app browser] was used to view a TikTok-owned website."[156]

According to its privacy policies TikTok automatically collects information about a user's approximate location based on a SIM or IP address and location information (such as tourist attractions, shops, or other points of interest) if users choose to add it to their user content. In some countries, such as Australia, South Korea and the USA, the most recent versions of the TikTok app do not collect precise or approximate GPS information.[157] Unlike in the other two policies (EEA/Switzerland/UK and the US), under its Other Regions policy, TikTok may collect precise location data (such as GPS) with a user's permission. TikTok claims that it uses location information to improve users' experience on the app, to show content that is popular in a user's area and where applicable, more relevant adverts.[158] This difference between the regional policies is an example of the ways in which TikTok applies uneven and therefore discriminatory privacy policies in different parts of the world.

TikTok states that the platform infers a user's attributes (such as age-range and gender) and interests based on the information it has about them in order to personalise and customise content (including in the 'For You' feed) as well as serve ads (including personalised/targeted ads where permitted). As outlined in Chapter 4, the inferring of user charateristics and interests involves an abuse of the right to freedom of thought, specifically the right to not reveal one's thoughts. Although TikTok's policy states that it infers age-range and gender, it is not clear if this is an exhaustive list of the attributes that it infers. Furthermore, a person's interests may overlap and reveal certain sensitive characteristics that they would not choose to reveal such as their sexuality or political affiliation.

153. Felix Krause, iOS Privacy: *Announcing InAppBrowser.com - see what JavaScript commands get injected through an in-app browser,* 18 August 2022, https://krausefx.com/blog/announcing-inappbrowsercom-see-what-javascript-commands-get-executed-in-an-in-app-browser)
154. Guardian, "TikTok can track users' every tap as they visit other sites through iOS app, new research shows", 24 August 2023, https://www.theguardian.com/technology/2022/aug/24/tiktok-can-track-users-every-tap-as-they-visit-other-sites-through-ios-app-new-research-shows
155. TikTok Newsroom, "TikTok Truths: A new series on our privacy and data security practices", 13 June 2023, https://newsroom.tiktok.com/en-us/tiktok-truths-a-new-series-on-our-privacy-and-data-security-practices
156. TikTok Newsroom, "TikTok Truths: A new series on our privacy and data security practices" (previously cited).
157. TikTok Newsroom, "TikTok Truths: A new series on our privacy and data security practices" (previously cited).
158. TikTok Newsroom, "TikTok Truths: A new series on our privacy and data security practices" (previously cited).

Under the Other Regions and US privacy policies (but not EEA/Switzerland/UK policy), TikTok also states that it collects this information "for demographic classification, for content and ad recommendations, and for other non-personally-identifying operations." Elsewhere, TikTok has clarified that "demographic classification" may include "inferred age range."[159]

Under the US privacy policy, TikTok "may collect biometric identifiers and biometric information as defined under U.S. laws, such as faceprints and voiceprints" from a user's content and will seek any required permissions from a user prior to any such collection where required by law. The vagueness of this part of the policy is concerning. It is not clear what the policy means by faceprints and voiceprints, how and when it will seek consent before taking this biometric information, or for what purpose TikTok will use this biometric data. It is also inherently contradictory that it includes "non-personally-identifying operations" as one of the purposes for collecting data, when biometric data is unique and can be used to identify someone. Nowhere else in the world does it collect biometric information where permitted by law and with user consent.

This update to TikTok's US privacy policy in June 2021 alarmed privacy experts, who were concerned about the permanence of biometric data, potential future uses of biometric data collected and vagueness in the policy around TikTok's intent given that the information is not essential to the functioning of the app. Furthermore, the ways in which TikTok can use the data collected under the privacy policy is broad and while TikTok states that it "does not sell your personal information or share your personal information with third parties for purposes of cross-context behavioral advertising where restricted by applicable law," it also says it may share the information it collects for "business purposes."[160] Moreover, there is no federal law restricting the sale or sharing of personal information with third parties for the purposes of cross-context behavioural advertising, though there are some state laws that restrict it. The policy states that TikTok will seek user permission for this type of data collection "where required by law," but doesn't specify whether it's referring to state law, federal law or both.[161]

Although there is no federal U.S. law regulating the collection and use of biometric data, some states have passed their own laws. Nevertheless, within the US it remains a legal grey area and opens the possibility that some users within the US may not be covered by legal protections reagarding their biometric data. Overall, this provision is concerning as it contains vague definitions of the data TikTok is collecting, how and why it needs to use it and is a risk to the right to privacy of US children on the TikTok app.

Additionally, TikTok uses cookies and similar tracking technologies to operate and provide the platform to users, including remembering a user's language preferences for security and marketing purposes. Under the EEA/UK/Switzerland policy however, TikTok must obtain a user's consent for the use of cookies where required by law. All countries in the EEA require website operators to obtain permission for cookies under the EU's GDPR. The UK and Switzerland have their own domestic legislation imposing this obligation.

TikTok's policy for the EEA/UK/Switzerland reflects the regulatory obligations imposed on it, but it results in users outside of the EEA, UK and Switzerland having less control over their data than users in that region. It is a clear example of how TikTok and many online companies only implement more privacy-respecting policies in response to regulation, but continue with less privacy-respecting practices where they can in a discriminatory manner.

159. TikTok Newsroom, "TikTok Truths: A new series on our privacy and data security practices," 13 July 2023, https://newsroom.tiktok.com/en-us/tiktok-truths-a-new-series-on-our-privacy-and-data-security-practices (accessed 27 September 2023)
160. Time, "What TikTok Could Do With 'Faceprints' and 'Voiceprints'", 14 June 2021, https://time.com/6071773/tiktok-faceprints-voiceprints-privacy/
161. The US privacy policy on the website has a link that says "Click here to learn more", but when researchers clicked the link, it led to an error page that said "Couldn't find this page" (last accessed on 18 October 2023)

Finally, TikTok also collects information from other sources including advertising, measurement and other partners about its users and the actions they have taken outside of the platform, such as their activities on other websites and apps or in stores, including the products or services they purchased, online or in person. These partners also share information with TikTok, which TikTok uses to help match a user and their actions outside of the platform with their TikTok account. Third-party platforms also provide TikTok with information when they choose to sign up for or log in to the TikTok app using sign-in features provided by those third parties, such as Facebook, Twitter, Instagram, or Google. In its response to Amnesty International's findings, TikTok wrote that the "TikTok app has its own built-in search engine functionality and does not directly collect what people search for outside of the app or through other search engines."[162]

Taken as a whole, TikTok collects a huge amount of data on each user, tracking them on the app and collecting information on their activity on the wider internet and in the physical world as well (for instance through location data and in store purchase data shared by partners), which many which users will not realise they are agreeing to when they sign-up for an account. The direct and indirect collection of this massive amount of data is a clear abuse of the right to privacy. Furthermore, comparing TikTok's three privacy policies and the data collected under each one reveals key differences particularly with respect to how much data is collected from users under in the EEA/Switzerland/UK and those subject to the Other Regions policy, which creates a discriminatory patchwork of policies.

HOW COLLECTED INFORMATION IS USED AND SHARED

TikTok states that it uses the information collected to customize and personalize the content that a user sees, particularly in the 'For You' feed. According to TikTok's three regional privacy policies it is also used to administer the platform, provide, and improve advertising services, to measure and understand the effectiveness of ads and other content, as well as to understand how people use the platform, in order to support its ongoing developmet.

Under sections relating to how user data is shared, there are some divergences between the three regional privacy policies. In EEA/UK/Switzerland, the policy states that TikTok will share data with advertisers and to provide advertisers with aggregate information about the performance of their ads and other content on the platform in order to help them measure their effectiveness. They also share a user's information directly with advertisers where a user gives their permission. TikTok also shares this data with measurement and data partners who help measure advertising served on the platform to help advertisers determine the effectiveness of their ads.[163]

The US privacy policy is less detailed on the sharing of information. Although under this policy, TikTok says that it "does not sell your personal information or share your personal information with third parties for purposes of cross-context behavioral advertising where restricted by applicable law", it does say that it shares the data with "service providers and business partners" including "advertising and marketing services"[164]

The Other Regions privacy policy has even less detail than the US policy. TikTok shares data with advertisers and third-party measurement companies to show how many and which users of the platform have viewed or clicked on an advertisement. Importantly, there is no statement that TikTok does not sell or share personal information with third parties for the purposes of cross-context behavioural advertising.

---

162. See Appendix to this report: Written response from TikTok, 29 October 2023.
163. TikTok, Privacy Policy (EEA/UK/Switzerland) (previously cited).
164. TikTok, Privacy Policy (US) (previously cited).

There is ambiguity regarding TikTok's sharing of information, especially with which third parties, and a lack of clarity as to whether users are notified if their information is transferred to a third party. This is of great concern given that in parts of the world covered by the Other Regions policy, TikTok processes children's data in the same way that it does adult users' data. Amnesty International wrote to TikTok to ask with which third-parties TikTok shares information and whether there were regional differences. Amnesty International also asked TikTok to share information on whether and when users are notified if their data is transferred to a third party. TikTok did not respond to this question.

The Other Regions policy also includes information on how the data of users on TikTok Lite is shared with advertisers and advertising and measurement partners. TikTok Lite is a smaller version of the app designed to be used where internet connection is less reliable and bandwidth is not as good. There is little information on the TikTok Lite app, but Tech Crunch reported in 2019 that the app had gained 12 million downloads within the first 6 months of its launch in 2018.[165] It is widely used in countries of the Global Majority. The policy states that TikTok "share[s] information with advertising networks to display personalised advertisements … on the TikTok Lite app and elsewhere online." However, the policy also says that TikTok is "not responsible for the privacy practices of these third parties, and the information practices of these third parties are not covered by this [TikTok's Other Regions] Privacy Policy." This is the clearest statement that it shares information with third-parties for the purposes of displaying personalised ads and there seem to be no restrictions on the sharing of users data on TikTok Lite for the purposes of advertising. The lack of restrictions on the sharing of TikTok Lite users' data is clearly discriminatory, as users of this app, which is only available in certain countries, have the least control over their data. This is similar to Facebook's Free Basics, a basic version of the Facebook app along with a limited number of services without incurring data charges on their mobile phones, which Amnesty International has previously found acts as a means for Meta to collect masses of data from people in the Global Majority.[166] A 2019 UN report found that with Meta's Free Basics, "more local data would mean opportunities for providing better targeted advertising."[167] Although Meta presents Free Basics as a philanthropic initiative providing an "onramp to the broader internet" for those who would otherwise lack internet access, Free Basics instead appears to be an "onramp" for increasing data mining in the Global Majority.[168]

In its written responses to Amnesty International's questions, TikTok stated that it does not sell or share users' personal information with third parties "for the purposes of cross-context behavioural advertising where restricted by applicable law." However, this suggests that TikTok may sell or share users' personal information with third parties for this purpose in countries where it is not prohibited by law. In a follow-up letter, Amnesty International asked TikTok whether this was the case, however TikTok did not respond to this question.

TIKTOK'S PRIVACY POLICY FOR CHILDREN UNDER THE AGE OF 13

The USA is unique in that it is the only country in which TikTok permits children under the age of 13 to create an account, using a curated, view-only app. TikTok has a separate privacy policy for them and this part of the platform.

---

165. In 2019, it was reported that there were two versions of the app covering different countries, but that together the two apps were available in India, Indonesia, Malaysia, The Philippines, Vietnam, Egypt, Brazil, Algeria, Tunisia, Russia, Ecuador, South Africa, Dominican Republic, Guatemala, Kenya, Costa Rica, El Salvador, Nigeria, Angola and Ghana. Tech Crunch, "TikTok's quietly launched 'Lite' app has reached over 12 million downloads since August" https://techcrunch.com/2019/01/04/tiktoks-quietly-launched-lite-app-has-reached-over-12-million-downloads-since-august/#:~:text=This%20version%20of%20TikTok%20Lite,installs%20since%20its%20August%20debut.
166. Amnesty International, *Surveillance Giants* (previously cited).
167. United Nations Conference on Trade and Development, Digital Economy Report 2019, September 2019, https://unctad.org/publication/digital-economy-report-2019, p 90.
168. Amnesty International, *Surveillance Giants* (previously cited).

In line with the US Children's Online Privacy Protection Act, TikTok collects much more limited information from under 13s, including username, password, and birthday, as well as some automatically collected device information according to its Children's Privacy Policy.[169]

TIKTOK'S ADVERTISING POLICIES AND PRACTICES

TikTok's advertising policies, practices, including profiling methods are based on the direct and indirect collection of large amounts of user data (as described above), which is used to create extremely detailed profiles of each user's interests which, in TikTok's words, allows them to "show you personalized ads, which are ads we think you will be interested in based on information we have about you."[170]

TikTok's advertising policies set out the type of products and services that can and cannot be advertised on the platform.[171]

According to these policies, TikTok may show ads to individual users based on the following information:

- General information: this includes location information (information based on users' approximate location) as well as device and network connection information;
- Demographic information: age and gender;
- In Tik-Tok activity: this is based on a user's activity on the platform, including information in relation to content and creators, enabling advertisers to target users based on their interests and behaviour on the platform;
- Off Tik-Tok activity: this is based on information shared by TikTok and by TikTok's advertising, measurement and data partners whose role is to help advertisers understand how their ads perform and based on user activity on their apps, websites or in person in their stores, to determine whether this user activity can be credited to a particular advertisement on TikTok.[172]

Users are thus tracked across the internet and even into the offline world (for example, through the collection of location data and in-person purchase data) to finely-tune the ad delivery service offered by TikTok, as well as prove the effectiveness of this ad delivery system in order to drive more advertising revenue.

HOW AND WHERE USERS CAN CONTROL ADS

TikTok's guide to "Ads and Your Data" explains how users can change how ads are personalized through adjusting their settings. However, the degree of control available to users depends on which region of the world they live in, creating regional differences between the extent to which users' right to control personal information is respected. TikTok said it "take[s] special care when crafting the experiences teens have on the platform, including the ads they see." However, it also admitted that some teen users are shown ads based on their activity both on and off the platform.[173]

In the EEA/UK/Switzerland region, users "can control personalization using your in-TikTok and off-TikTok activity for the ads that you see" and, additionally to adjust their preferences to see more relevant advertisements using the ad interest options. Both features are only available in this region.

169. TikTok, Children's Privacy Policy, https://www.tiktok.com/legal/page/global/privacy-policy-for-younger-users/en (updated 1 January 2023)
170. TikTok, "Ads and Your Data", https://www.tiktok.com/safety/en/ads-and-data/ (accessed on 7 March 2023). Page no longer available.
171. TikTok, Advertising Policies, https://ads.tiktok.com/help/article/tiktok-advertising-policies-ad-creatives-landing-page?redirected=2 (accessed on 22 May 2023).
172. TikTok, "Ads and your data", https://www.tiktok.com/safety/en/ads-and-data/ (accessed on 7 March 2023).
173. See Appendix to this report: Written response from TikTok, 12 July 2023.

Whereas, outside the EEA, the UK and Switzerland, including in the US, users can only change how data about their off-TikTok activity is used for ads personalization, but cannot control the use of data collected from their in-TikTok activity, hence the ads that they receive are always based on individual user activity on the platform.

Users in all regions can adjust their settings in IOS and Android devices to alter the way ads are targeted at them. Where the former allows a user to stop tracking activities across other companies' apps and websites, the latter allows for the user to delete or pause the advertising ID[174] which affects the ads' personalization.

In June 2023, TikTok told Amnesty International that it would start "restricting the types of data that can be used to show ads to teens by region."[175] According to its revised policies, in Europe (EEA/UK/Switzerland) users between the ages of 13 to 17 will no longer see personalized ads on TikTok based on their activities both *on* or *off* TikTok.[176] However, recent research from Stiftung Neue Verantwortung has cast doubt on whether TikTok has followed through on its July 2023 announcement that minors in the EEA/Switzerland/UK would no longer be targeted based on their on and off TikTok activity.[177] Amnesty International asked TikTok to confirm whether the company has indeed followed through on its July 2023 announcement that minors in the EEA/Switzerland/UK would no longer be targeted based on their on and off TikTok activity. In response, TikTok wrote that "[t]his policy has been implemented and we will continue to move toward providing our community with transparency and controls so they can choose the experience that's right for them."[178] In the USA, users aged between the ages of 13 and 15 will no longer be targeted with personalised ads on TikTok based on their activities *off* TikTok. This means that in the USA, teenagers aged 16 and 17 will continue to be targeted with personalized advertising based on their activity both *on* and *off* TikTok, including the websites they visit, the places they go and so on, and younger users aged between 13 and 15 will continue be targeted based on their *on* TikTok activity i.e. they are still targeted with behavioural advertising with only slight modifications made for younger users. More worryingly still, users under the age of 18 who live in countries covered by TikTok's Other Regions privacy policy, will continue to be shown ads based on both their *on*- and *off*-TikTok activity.

It is clear that TikTok announced the restrictions on targeted advertising for users under the age 18 in Europe in response to the obligations that were due to be imposed on it when the DSA came into force in August 2023. TikTok's approach is to implement more data extractive policies in countries and regions with weaker laws and regulation, as well as weaker enforcement, and thus offers a less privacy-respecting app and experience to users under the age of 18 outside of the EEA/UK/Switzerland region.

By implementing less extractive and invasive privacy policies and data practices for child users in Europe, TikTok's policies are inherently discriminatory and TikTok is failing in its responsibility to respect child users' right to non-discrimination in large parts of the world.

AD TARGETING

This section outlines how advertisers can target ads to specific categories of users based on information collected, processed, and aggregated, including inferences based on machine learning, by TikTok.

174. An advertising ID is a unique user ID assigned to a mobile device, or operating environment, to help advertising services personalize their offers. It can be sent to advertisers and other third parties which can use this unique ID to track the user's movements, activity on, and engagement with applications.
175. See Appendix to this report: Written response from TikTok, 12 July 2023
176. TikTok subsequently announced this publicly in August 2023, TikTok Newsroom, "An update on fulfilling our commitments under the Digital Services Act", https://newsroom.tiktok.com/en-eu/fulfilling-commitments-dsa-update (accessed 17 August 2023)
177. Auditing TikTok, *Ad-Targeting for minors still exists but it shouldn't, 28 August 2023*, https://tiktok-audit.com/blog/2023/ads-targeting-minors/
178. See Appendix to this report: Written response from TikTok, 29 October 2023.

TikTok offers a variety of different metrics that advertisers can use to target their ads at users of the platform, including the following:

- Location targeting that enables advertisers to tailor messages and offer products and services to specific locations.[179]
- Interest targeting that enables advertisers to target individuals based on categories related to their long-term interests, such as education, beauty, skincare etc.,[180] and interaction with content on TikTok, which is based on predictions through machine learning based on long-term past behaviour and key indicators.[181]
- Behaviour targeting which focuses on a user's recent engagement with content. TikTok classifies behaviour into two categories: video-related actions which includes likes, shares and comments on video content in the last 15 days; and creator-following behaviour which targets users who follow specific types of creators or have viewed certain types of creator profiles in the last 30 days.[182]
- Hashtag targeting, which is a type of behavioural targeting, that enables advertisers to target users who watched TikTok videos with certain hashtags.[183]
- Purchase Intent Targeting enables advertisers to target users that are actively searching for a specific category or product or service on TikTok, interacting with content about a product or service through likes, shares etc. or users who were close to completing a purchase.

TikTok provides recommendations to advertisers on which categories of users to target to help them identify their target audiences, as well as analyses the performance of similar ads from comparable advertisers along with the performance of ads already posted by advertisers.

In addition, TikTok also provides advertisers with two other ad targeting options, Custom and Lookalike Audiences. Custom Audiences enables advertisers and businesses to find people who already know or have previously engaged with their business.[184] Lookalike Audiences enables them to identify audiences that share common interests or attributes with their existing customers. Lookalike audiences are created by using algorithms which study the attributes of a custom audience created by an advertiser or a business. TikTok's algorithm analyses attributes of the users from the Custom Audience type selected, such as demographics, location, operating system, interests, etc. and then looks for other users and groups who share similar attributes that can be targeted with an advert.[185]

As explained above in Chapter 2, although lookalike audiences change the advertising delivery model so that advertisers do not specify a list of attributes or interests that they want to use to target users, the algorithm creates a lookalike audience that will be targeted by making predictions about the individual users in a lookalike audience group and their personal attributes, common interests and information, some of which will be sensitive.[186] This model thus still has the same implications for human rights as

179. TikTok Business Help Center, "About Location Targeting", https://ads.tiktok.com/help/article/location-targeting?lang=en (accessed on 23 May 2023)
180. TikTok Business Help Center, "About Interest Targeting", https://ads.tiktok.com/help/article/interest-targeting?lang=en (accessed on 23 May 2023)
181. TikTok Business Help Center, "About Behavior Targeting", https://ads.tiktok.com/help/article/behavior-targeting?lang=en (accessed on 23 May 2023)
182. TikTok explains the different between Interest Targeting and Behaviour Targeting thus: "Interest Targeting is developed based on Machine Learning, while Behaviour Targeting captures the ground truth behavior of the user." TikTok Business Help Center, "About Behavior Targeting" (previously cited).
183. TikTok Business Help Center, "About Behavior Targeting" (previously cited).
184. TikTok Ads Manager, "About Custom Audiences", https://ads.tiktok.com/help/article/custom-audiences?lang=en (accessed 23 May 2023)
185. TikTok Ads Manager, "About Lookalike Audience", https://ads.tiktok.com/help/article/lookalike-audience?lang=en (accessed on 23 May 2023)
186. For instance, Article 9 of the EU and UK GDPR establishes special categories that require extra attention. Sensitive data, or special category data, according to GDPR is any data that reveals a subject's information. Sensitive data examples: racial or ethnic origin, political beliefs, religious beliefs, genetic or biometric data, mental health or sexual health, sexual orientation and trade union membership.

targeted personalized advertising, which is based on inferences about individual users' interests and constitutes an invasion of the rights to privacy and freedom of thought.

TikTok states that it does not use sensitive personal data, as defined by the EU and UK GDPR, to personalize content, nor does it use machine learning to draw inferences about protected characteristics[187] beyond gender and age-range from data collected from users. However, it does group people according to their behaviour and activity online, which may without a user's knowledge, overlap with and reveal certain protected characteristics that constitute sensitive personal data. For instance, people interested in baby products, who are likely to be expectant parents, including pregnant women and birthing people may be targeted with baby-related content or excluded from seeing other adverts, or people signalling an interest in LBGTI+ content could be taken as proxy for their sexuality.

According to a health marketing agency, healthcare advertisers wishing to advertise on TikTok are offered the following sub-categories; dietary supplements, medicine, medical information, other health and medical services. Examples of some of the hashtags that are available as targeting categories are #backpain and #ivfbaby. Furthermore, healthcare advertisers can create lookalike or custom audiences based on lists of existing patients, which then allows TikTok to find users that are similar. These advertising services pose an obvious risk to the right to privacy, as hashtags that users search for may reveal their medical conditions, and of those on the lookalike list whose medical conditions may be inferred in being clustered together in the lookalike group.[188]

In May 2023, the Wall Street Journal reported that, according to former employees of TikTok, lists of users who watched LGBTIQ+ content on the app were visible to some staff. Although TikTok does not ask users to disclose their sexual orientation, videos can be tagged as LGBT and the profile names of users who watched those videos could be seen by some employees on a dashboard. In response, TikTok said that the dashboard had been deleted nearly a year prior to the Wall Street Journal's report, and that TikTok does not identify or infer sensitive information such as the sexual orientation or race of users based on their watch history.[189] Nevertheless, this report shows how compiling a list of people who show an interest in particular topics and watch certain related content can potentially reveal certain sensitive information about people, which is then provided to businesses as categories of people at which they can target their advertising.

While the algorithm that delivers targeted ads and content may not be programmed to infer mood, sexuality etc. if people are grouped according to interest group, TikTok can still create incredibly detailed profiles of each user according to the categories in which they are clustered and which can serve as proxies for sensitive information that can then be used to target them with ads and thus make profit. For instance, users signalling an interest in #sadtok will be targeted with content that the algorithm predicts will appeal to them. While it may not be creating a list of users grouped together by mood, the interests and hashtags can still thus reveal intimate details about their mood. Thus, the impact on human rights is the same. It's important to point out that the inferences do not need to be correct to have an impact on human rights. Incorrect sensitive inferences and misclassification can also have an adverse impact on human rights.

A ruling by the Court of Justice of the European Union confirmed this when it found that inferred sensitive/protected data are sensitive/protected data under Article 9 (Processing of special categories of

187. Protected characteristics under many jurisdictions equality legislation include: age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, sexual orientation.
188. Runner Agency, TikTok Advertising for Healthcare - A Guide, 22 November 2022 https://runneragency.com/blog/tiktok-advertising-healthcare/
189. Wall Street Journal, "TikTok Tracked Users Who Watched Gay Content, Prompting Employee Complaints", 5 May 2023, https://www.wsj.com/articles/tiktok-tracked-users-who-watched-gay-content-prompting-employee-complaints-5966a5f5)

personal data) of the EU GDPR.[190] This judgement could have far-reaching consequences and change the status quo around algorithmic recommender systems and online advertising in the EU that national data protection authorities will be able to use to rein in the extractive data practices of Big Tech, including social media platforms.

It is particularly troubling that in many parts of the world children over the age of 13's data is treated the same as adults' data, and therefore this level of protection is lacking.

TIKTOK'S ANTI-DISCRIMINATION AD POLICY

TikTok's "Anti-discrimination Ad Policy" prohibits advertisers from using TikTok's ad products to discriminate against people wrongfully either by targeting or excluding specific groups of people. According to TikTok's written responses to Amnesty International, advertisers "may not include any unlawfully discriminatory or harassing content in their advertising or any content that encourages unlawful discrimination or harassment."[191]

TikTok's policy explicitly prohibits advertisers from using audience selection tools to "(a) wrongfully target specific groups of people for advertising in a way that breaches applicable laws or regulations; or (b) wrongfully exclude specific groups of people from seeing their ads, in breach of applicable laws or regulations." It prohibits advertisers from targeting or excluding specific categories of users – notably "legally protected classes based on the local laws of the region, such as race, ethnicity, age, familial status, and sexual orientation." It also prohibits targeting or excluding users on the basis of:

- "National identity, country of citizenship, country of origin, or veteran status or identity or beliefs in regards to political groups, religion or union affiliations;
- Personal, financial, or legal hardships;
- Individual health statuses or disabilities, including mental, physical, genetic, or emotional health and conditions".[192]

Under TikTok's anti-discrimination ad policy, while it provides advertisers and businesses with the information and tools to enable them to target audiences, it leaves it to them to ensure that they comply with applicable local anti-discrimination laws and regulations, for example, laws or regulations which make it illegal to offer housing, employment, or credit to certain categories of people only.[193]

However, as discussed above, certain interest categories can overlap with or reveal sensitive personal information or can be used as proxies for protected characteristics and be used to target people or exclude them.

TikTok's anti-discrimination policy states that advertisers should work with its representatives on specific country or regional legal nuances, and that as the company develops new products, features, and services, it may include additional targeting restrictions as required by applicable laws and regulations.[194]

It is not clear whether TikTok has any procedures for identifying whether or not advertisers on its platform are complying with local laws on equality and anti-discrimination (where they exist) or whether or how it assesses the risk that they might be using tools and data provided by TikTok to discriminate in favour or against certain categories of people. Neither is it clear what action TikTok would take

190. Judgement of 1 August 2022, *OT vs Vyriausioji tarnybinės etikos komisija*, C 184/20, ECLI:EU:C:2022:601, https://curia.europa.eu/juris/document/document.jsf?text=&docid=263721&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=481514
191. See Appendix to this report: Written response from TikTok, 12 July 2023.
192. Business Help Center, "TikTok's anti-discrimination ad policy" (previously cited).
193. Business Help Center, "TikTok's anti-discrimination ad policy" (previously cited).
194. Business Help Center, "TikTok's anti-discrimination ad policy" (previously cited).

should the company find that an advertiser or business is unlawfully targeting or excluding certain groups. Amnesty International wrote to TikTok and asked whether the company audits or in any way checks that advertisers are complying with laws related to equality and discrimination where they exist, as well as what action TikTok takes if it discovers that an advertiser is using the platform tools in a discriminatory manner. In response, TikTok disagreed with Amnesty International's assessment of the company's enforcement of its Anti-Discrimination Ad Policy and wrote that "[a]ll advertisements on TikTok are subject to our Community Guidelines and Advertising Policies. As a result, advertisements are not permitted if they violate TikTok's policies. Although TikTok's Advertising Policies detail what kinds of products and services are prohibited and restricted, including a prohibition on ads that "that discriminates or harasses, encourages discrimination or harassment, or includes hate speech against protected groups, individuals, or organizations based on protected personal characteristics, including, but not limited to, race, ethnicity, national origin, sexual orientation, gender identity, religious affiliation, age, family status, medical or genetic condition",[196] TikTok did not respond to Amnesty International's questions about how it ensures that advertisers are complying with local laws on ad targeting where the content of the ad is not prohibited, restricted or discriminatory.[197]

Although no examples of such discrimination were found in the research for this report, this apparently hands-off approach by TikTok means that there is a risk that advertisers could discriminate against certain categories of people through targeting or exclusion.

> ***"Personal data collection is something I'm uncomfortable with, but I've sadly gotten used to it....***
>
> ***The cost of using most mainstream social media platforms appears to be my privacy. My tastes and interests are constantly monitored by powerful and wealthy corporations against which I feel powerless.***
>
> ***While I understand the legal requirement to have solid and precisely defined terms of service, the way in which they are presented is intentionally hard to read and understand by most users. This way, most users just don't bother. Especially not when they are just starting to use a platform."***
>
> 21, "Antonio", Argentina, 2022

7.2 MEASURES TAKEN BY TIKTOK TO ADDRESS PRIVACY AND DATA PROTECTION CONCERNS

DUE DILIGENCE

In order to assess whether TikTok has conducted adequate human rights due diligence in line with international standards and taken adequate steps to mitigate and prevent the risks and abuses to the rights to privacy, freedom of thought and non-discrimination, this section will assess its policies and practices against the six-step due diligence framework outlined in OECD Due Diligence Guidance for Responsible Business Conduct, outlined below.[197]

1. Embed responsible business conduct into policies and management systems;
2. Identify and assess adverse impacts in operations, supply chains and business relationships;

195. TikTok Business Help Center, TikTok Advertising Policies - Ad Creatives and Landing Page: Prohibited Content, https://ads.tiktok.com/help/article/tiktok-advertising-policies-ad-creatives-landing-page-prohibited-content?lang=en
196. See Appendix to this report: Written response from TikTok, 29 October 2023.
197. OECD, Due Diligence Guidance for Responsible Business Conduct (previously cited).)

3. Cease, prevent or mitigate adverse impacts;
4. Track implementation and results;
5. Communicate how impacts are addressed; and
6. Provide for or cooperate in remediation, when appropriate.

The first step is to embed responsible business conduct into polices and management systems. To this end, it is essential that a company has a human rights policy, which references the UN Guiding Principles on Business and Human Rights (UN Guiding Principles)[198] and someone at senior management level who is responsible for overseeing its implementation. In its written response to Amnesty International, TikTok stated that its approach to youth safety is informed by its commitment to human rights, in particular the UN Guiding Principles on Business and Human Rights (UN Guiding Principles).[199] However, although it publicly commits to respecting human rights on its website, TikTok does not have a publicly available human rights policy. Amnesty International wrote to TikTok to ask whether the company has such a policy, which covers a broad range of human rights including the rights to privacy, freedom of thought and health, and whether it is publicly available. Amnesty International also asked who within the senior management of the company is responsible for its implementation. TikTok responded by pointing Amnesty International to the human rights commitment on their website, which is informed by a number of international human rights frameworks including the UN Guiding Principles, which the company has pledged to uphold. However, TikTok did not share a human rights policy as requested by Amnesty International nor information on who at a senior level is responsible for its implementation and how it is embedded from the top of the company through all its functions.[200]

TikTok did state in its written response to Amnesty International that it has a centralized team that leads its human rights work, as well as other staff throughout the company who it says are "empowered by leadership to address any identified risks." Amnesty International asked TikTok how large this team is and who on the senior management they report to. Amnesty International also asked how these staff are empowered to address any identified risks, what process is in place when staff identify a risk, and what action they can take. TikTok did not respond to this question.[201]

The second and third steps involve identifying and assessing adverse impacts in operations, supply chains and business relationships and ceasing, preventing, and mitigating any actual and potential adverse impacts that are identified.

TikTok's Community Guidelines also include a sub-section on its policies on youth safety and well-being which are overseen by a sub-team in the Trust and Safety Product Policy team. Additionally, its "Platform Fairness team specializes in issues of human rights, fairness, and inclusion and applies a multifaceted approach to the review and revision of policies, product features, and algorithmic systems."

TikTok did not provide details in its letter to Amnesty International about what this "multi-faceted approach" entails, in what way it reviews or revises policies, product features or algorithmic systems or what specific risks the company is looking for or has identified, in particular in relation to its data collection practices and recommender system.

TikTok explained in its letter to Amnesty International that its teams, which according to the company includes youth safety experts, proactively assess human rights risks related to young people but did not provide any details about how this is done.

198. See Appendix to this report: Written response from TikTok, 12 July 2023.
199. See Appendix to this report: Written response from TikTok, 12 July 2023.
200. See Appendix to this report: Written response from TikTok, 29 October 2023.
201. See Appendix to this report: Written response from TikTok, 29 October 2023.

TikTok did not provide a list of risks that it had identified, and it is unclear how potential risks to users', and specifically children's rights, are identified. In particular, it is not clear if the company has identified risks relating to the right to privacy and freedom of thought arising from its data collection practices, profiling and recommender algorithm systems. Amnesty International could not find any information on what measures TikTok has in place to prevent abuses and mitigate any such risks on the company's website.

TikTok did not include a list of specific risks identified nor steps that it has taken to prevent and mitigate them in either of its written responses. Amnesty International specifically asked TikTok whether the company had identified risks to children (people under the age of 18) inherent in the design of its platform and/or its data collection, user profiling and advertising practices, especially in relation to the right to privacy, the right to freedom of thought, the right to non-discrimination and if so, how these risks were identified and what actions were taken to prevent these harms or mitigate them. TikTok did not respond to this question.

However, TikTok did say that it has embedded a human rights approach across its community guidelines, that it has global advisory councils which include experts in children's rights and is a member of the "WeProtect Global Alliance and the Tech Coalition", where it engages with its peers on current and upcoming risks.[202] In June 2023, TikTok also announced the creation of a Youth Council, which it says will provide "a more structured and regular opportunity for young people to provide their views." In its 29 October letter, TikTok states that it is "working to build the council with youth representing a diversity of backgrounds and geographies."[203]

These initiatives have the potential for greater, ongoing engagement by TikTok with rightsholders, experts, civil society organizations and other stakeholders. However, it remains unclear exactly how this engagement will inform TikTok's due diligence and risk assessments and how frequently and meaningfully stakeholders will be consulted.

Given the lack of information on risks identified and prevention and mitigation strategies, it is unclear whether TikTok is undertaking due diligence in line with international standards.

Although TikTok has never publicly acknowledged the human rights risks that child users of the platform face, particularly associated with its business model and data collection practices, it has nevertheless introduced tools that seem to be informed by the possibility that such risks to children's rights exist.

In its written response, TikTok stated that the company applies safety-by-design principles in the design of its platform and that user safety is a priority throughout the product and feature development decision-making processes. It explicitly noted that it aims to promote a safe and age-appropriate experience for teens aged 13 to 17 in the design of its tools and policies and set out a range of measures that it has taken to protect children.

TikTok has a 'youth portal' on its website, which includes information for younger users on topics such as how to control who sees their videos, how to keep their account secure using a strong password, how to limit unwanted comments and how to take action on bullying online.[204] However, it does not provide information on how TikTok uses younger users' data. Research conducted on the TikTok platform for *Driven into Darkness* showed that teen accounts were occasionally shown explainer

202. WeProtect Global Alliance is a global multi-stakeholder group set up to develop policies and solutions to protect children from sexual exploitation and abuse online. WeProtect Global Alliance, "Who We Are", https://www.weprotect.org/about-us/who-we-are/ (accessed 27 September 2023). Tech Coalition describes itself as an alliance of global tech companies, who are working together to combat child sexual exploitation and abuse online. Tech Coalition, About, https://www.technologycoalition.org/about (accessed on 27 September 2003).
203. See Appendix to this report: Written response from TikTok, 29 October 2023.
204. TikTok, "Youth portal", tiktok.com/safety/youth-portal?lang=en

videos explaining how their data was collected and used.[205] Amnesty International asked TikTok what languages this video explainer is available in and how often it is shown, but TikTok did not respond to this question.

While TikTok has provided some information on the design features that it has implemented to create safe and age-appropriate experiences for teen users, which are welcome, TikTok has not disclosed information related to which risks they have identified that these strategies are seeking to address. Furthermore, TikTok is primarily focused on issues related to protecting children against certain harmful content or potentially harmful contact with other users through keeping their accounts secure and ensuring default privacy settings for younger users. It does not, however, address the abuse of the rights to privacy and freedom of thought that underpin TikTok's business model.

The fourth and fifth steps in the OECD Due Diligence Guidance are to track implementation and results and communicate how impacts are addressed. The UN Guiding Principles make clear that, in accounting for how they address their human rights impacts, businesses should have "in place policies and processes through which they can both know and show that they respect human rights in practice."[206] The UN Guiding Principles also clarify that showing that a company respects human rights "involves communication, providing a measure of transparency and accountability to individuals or groups who may be impacted".[207]

Amnesty International could not find any information about TikTok's human rights due diligence policies and processes on its website or in its publicly available documents. In its response to Amnesty International, TikTok states that it plans to conduct periodic impact assessments in partnership with third parties, which may take the form of company-wide assessments, team assessments and product or business line specific assessments.[208]

Amnesty International requested details from TikTok about the company's human rights due diligence policies and practices. TikTok responded in October 2023 that it "consults with a range of stakeholders to inform our human rights due diligence and are in the process of implementing a number of recommendations to our trust and safety operations that have resulted from our engagement with Article One Advisors on human rights. These recommendations are implemented by our platform fairness team in partnership with a human rights working group of colleagues on teams across the company. The assessment recommended that TikTok to conduct [sic] a child rights impact assessment, which we will be launching in partnership with Article One."

While it is positive that the company has a human rights working group made up of staff on teams across the company and that TikTok will be conducting child rights impact assessments, the fact that it has not to date implemented such impact assessments given the huge popularity of its platform with under 18s is a considerable oversight. It is questionable whether TikTok has been able to adequately assess the risks posed to children by its platform without such impact assessments and reflects a failure to carry out due diligence adequately.

Indeed, TikTok states in its letter to Amnesty International that another recommendation is to "develop a company-wide human rights due diligence process which will include conducting periodic human rights impact assessments", which the company is in the process of developing and "which will propose the triggers around when we need to conduct an assessment." That TikTok currently does not have a human rights due diligence process in place is a clear failure of the company's responsibility to

205. *Driven into Darkness*
206. UN Guiding Principles (previously cited), Principle 21 and commentary.
207. UN Guiding Principles (previously cited), Principle 21 and commentary.
208. See Appendix to this report: Written response from TikTok, 12 July 2023.

respect human rights. It is also not clear what it means by triggers that will show when an assessment needs to be conducted. Given the serious risks to children's human rights posed by the platform, the huge numbers of children that use the platform globally and the importance that it has in many children's lives, it is imperative that the company conducts child rights impact assessments both regularly as part of its due diligence and whenever it implements new design features.

It is not clear from either of TikTok's responses how the assessments they reference will be conducted, and these do not appear to have started yet. Amnesty International wrote to TikTok to ask when these assessments will begin, how TikTok will ensure that these impact assessments are integrated into a human rights due diligence process in line with international standards on business and human rights and how TikTok intends to ensure that the recommendations from those impact assessments are implemented. Amnesty International also requested information on whether these assessments would be made public. TikTok did not respond to this question, nor did it share any information on whether the child rights impact assessments or periodic human rights impact assessments, as part of the due diligence process that the company is in the process of developing, will be made public. Nor has TikTok disclosed any information on the frequency of these assessments and whether it will be publishing reports on the outcome of its due diligence process.

TikTok is thus not carrying out adequate human rights due diligence and failing in its responsibility to respect human rights, as laid out in the UN Guiding Principles.

8. CONCLUSION AND RECOMMENDATIONS

TikTok's highly personalized 'For You' feed has helped it to become, in the space of a few years, one of the most popular social media platforms in the world with over 1 billion users, many of whom are children between the ages of 13 and 17. But behind the never-ending feed of lip-syncing and dance craze videos is a highly extractive business model predicated on the direct and indirect collection of massive amounts of personal data – some of which is sensitive – on each user's behaviour on the platform and in some parts of the world, their activity off the platform, as well as in the physical world.

TikTok then uses this data to create profiles of users based on the data collected and inferences about each user, which it can cluster in groups to target them with highly personalized content and ads – a practice which is inconsistent with the rights to privacy and to freedom of thought and poses risks to a range of other human rights, including the right to non-discrimination. It is unclear what specific risks and abuses TikTok has identified, particularly in relation to its data collection practices and business model, and what mitigation and prevention strategies it has implemented in response, as TikTok is not carrying out human rights due diligence in line with international standards

To the extent that policies and practices have been put in place to ensure greater respect of children's rights, they differ from region to region. Hence, teenage users in Europe, where regional and national regulatory frameworks are the strongest, are afforded the greatest privacy-respecting policies and practices. In the USA young users have some, but fewer protections than their European counterparts. However, elsewhere in the world, where laws and regulations relating to data protection are often weaker, TikTok's "Other Regions" policy, allows for the most extractive data practices, with the result that children's on and off-line actions are being tracked and inferences drawn about them, so that they can be targeted with behavioural advertising. This differential treatment for child users in some parts of the world is discriminatory and TikTok should immediately extend the same rights-respecting policies to all child users globally by not allowing targeted behavioural advertising for any users under the age of 18.

This does not mean that the rights of children in Europe are fully respected. All TikTok users, including those under the age of 18, are targeted with highly personalized content via their 'For You' feeds, which is the defining feature of TikTok, based on inferences about them including their mood, interests and sensitive personal characteristics such as an interest in baby products and LGBTI+ issues. The business model of TikTok thus constitutes a massive invasion of the right to privacy and an abuse of freedom of thought and opinion with potential serious knock-on impacts on the right to non-discrimination and a range of other rights.

This is of concern in general, but particularly in relation to the many millions of children using TikTok, as not only can children not grasp the consequences of privacy violations taking place at scale, but

the difficulty of understanding social media platforms' terms of service calls into question whether their agreement to them can be considered genuinely informed consent. Creating spaces online in which children's rights to privacy and freedom of thought are important, as these rights are essential in the development and formation of their identities. Given the negative impacts on human rights of TikTok's current business model, the platform cannot be acting in children's best interests.

This report adds to Amnesty International's previous research that shows that Big Tech companies are either unwilling or incapable of addressing the negative human rights impacts of their surveillance-based business model in the absence of effective regulation. The failure of TikTok to put in place adequate policies to respect the rights of children makes it clear that stronger laws and regulation on data protection and algorithmic amplification of content on social media, and effective enforcement of such laws and regulation, are needed in order to keep children safe from the harvesting and exploitation of their personal data for profit.

It also requires a complete transformation of the business models on which TikTok, and other social media companies, have built their businesses. The internet does not need to depend on mass surveillance. Indeed, the widescale abuses of rights to privacy and freedom of thought and opinion are not inherent to online services. Rather, they arise from deliberate design decisions which are aimed at enabling TikTok to grow its user base and profits.

Despite some positive signs that national and regional law makers are looking to rein in Big Tech and ensure stronger protections for children on social media platforms, even the EU's progressive General Data Protection Regulation and Digital Services Act do not go far enough to address the underlying abusive business model. Given the irrefutable evidence of harms being caused to children by the invasive practices of TikTok and other social media companies (see companion to this report, Driven into Darkness), it is essential that states move quickly to introduce and enforce comprehensive laws to rein in their surveillance-based business models and associated business practices.

RECOMMENDATIONS

RECOMMENDATIONS FOR TIKTOK

- If it has not already done so, TikTok should develop a human rights policy consistent with the UN Guiding Principles on Business and Human Rights and in consultation with human rights and child rights experts, and with children from all regions of the world. The policy should be made publicly available without delay.
- TikTok should immediately stop allowing advertisers to target children around the world under the age 18 with personalized ads based on their on and off-TikTok activity, as it has done in the EEA, the UK and Switzerland.
- TikTok (and other technology companies that depend on invasive data-driven operations amounting to mass corporate surveillance) must rapidly transition to a more rights-respecting business model. As a first step, TikTok must put in place effective due diligence policies and processes and ensure that these address the systemic human rights abuses associated with the business model including the way in which it undermines the rights to privacy, and to freedom of opinion and thought. They must be transparent about the risks, including to human rights, that they have identified and how they have been addressed.
- To protect people's privacy and to give them real choice and control, a profiling-free social media ecosystem should not be an option but the norm. Content-shaping algorithms used by TikTok

should therefore not be based on profiling (e.g. based on watch time, engagement etc.) by default and must require an opt-in instead of an opt-out. Consent for opting in should being freely given, specific, informed, (using child-friendly language), and unambiguous.

- TikTok should cease collecting intimate personal data and drawing inferences from a user's watch time and engagement about their interests, emotional state or well-being for the purposes of personalizing content recommendations and ad targeting, which undermine the right to privacy and threaten the rights to freedom of thought and opinion and the right to health. Rather than using surveillance to identify and adapt feeds to user interests, TikTok should enable interests to be communicated by users through deliberate prompts (e.g. users could be asked to enter specific interests if they would like to be served personalized recommendations) and only when based on users' freely given, specific and informed consent.
- TikTok must undertake human rights due diligence in line with international standards and demonstrate that it is doing so, by identifying, preventing, mitigating and accounting for how they address its actual and potential impacts on human rights.
- TikTok must engage children and young people, academic and civil society experts and other relevant stakeholders in its ongoing human rights due diligence processes. Children and young people should also play a core part in implementing "safety by design" by being involved in the development process of tools and features of social media platforms.
- Human rights impact assessments should be published on a regular basis and should include detailed information on risks and mitigating measures taken with respect to specific countries (especially where systems may have a greater impact due to political conflicts or humanitarian emergencies), specific categories of users such as children and young people, and specific product changes.

RECOMMENDATIONS FOR STATES

Recommendations for meaningful data protection and platform regulation.

States must:

- Ensure that access to and use of essential digital services and infrastructure such as TikTok and other social media platforms are not made conditional on ubiquitous surveillance of children, young people or adult users. This will require enacting and/or enforcing comprehensive data protection laws in line with international human rights law and standards to prohibit targeted advertising on the basis of invasive tracking practices. These laws should restrict the amount and scope of personal data that can be collected, strictly limit the purpose for which companies process that data and ensure inferences about individuals drawn from the collection and processing of personal data are protected. They should further require that companies provide clear information to their users about the purpose of collecting their personal data from the start and that they do not further process it in a way that is incompatible with this purpose or their responsibility to respect human rights.
- As a first step, prevent companies from making access to their service conditional on individuals 'consenting' to the collection, processing or sharing of their users' personal data for content targeting and marketing or advertising.
- Regulate social media companies to ensure that content-shaping algorithms used by online platforms are not based on profiling by default and that they require an opt-in rather than an opt-out, with the consent for opting in being freely given, specific, informed and unambiguous.

The collection and use of inferred sensitive personal data (for example, recommendations based on watch time and likes which allow for inferences of sensitive information) to personalize ads and content recommendations must be banned. Rather, users should be in control of which signals or declared interests they want the platform to factor into the shaping of their feed. For those who prefer a feed based on personalized recommendations, they must be given the option to communicate personal interests to the platform based on specific, freely given and informed consent and based on prompts made in child-friendly language.

- Regulatory processes must involve meaningful consultation of affected groups, including children and young people, as well as independent experts and civil society organizations.
- Ensure that independent national data protection regulators are established, that their independence is guaranteed in law and that they have adequate resources, expertise and powers to meaningfully investigate and sanction abuses of regulations by social media companies in line with international human rights law and standards. They must be able to ensure independent and effective oversight over platform design as well as the design, development and implementation of algorithmic systems to ensure companies are held legally accountable for the identification, prevention and mitigation of human rights harms linked to such systems.
- Enact or enforce regulatory frameworks to ensure people are able to exercise in practice their right to choose privacy-respecting alternatives to surveillance-based business models. This includes measures to ensure interoperability (the ability to communicate with existing contacts using another compatible platform) rather than just data portability so that people can move between services without social detriment, and to lessen network effects.
- Require TikTok and other social media companies to provide age-appropriate explanations to children, or to parents and caregivers for very young children, of their terms of service. For children, these should use clear and simple language, provide transparent information throughout the user process and not only at the beginning, and provide clear explanations of user control choices and default settings. Social media companies should also be required to provide non-textual measures to aid understanding of their terms of service, such as images, videos and animations, and they should be easily contactable for any questions.
- Make the best interests of the child a primary consideration when regulating advertising and marketing addressed to and accessible to children. Sponsorship, product placement and all other forms of commercially driven content should be clearly distinguished from all other content and should not perpetuate discriminatory stereotypes (such as those based on gender, race, age, disability etc.).

Recommendations for human rights due diligence.

States must:

- Require by law that technology companies carry out ongoing and proactive human rights due diligence to identify and address human rights risks and impacts related to their global operations, including those linked to their algorithmic systems or arising from their business model as a whole. Where businesses target children or have children as end users, they should be required to integrate child rights into their due diligence processes, in particular to carry out and make publicly available child rights impact assessments, with special consideration given to the differentiated and at times severe impacts of the digital environment on children. They should take appropriate steps to prevent, monitor, investigate and punish child rights abuses by businesses.

Recommendations for effective remedies.

States must:

- Invest in, encourage, and promote the implementation of effective digital educational programmes to ensure that children understand their rights, including their right to seek an effective remedy against any data protection, privacy or other human rights abuse, when accessing digital services.
- Guarantee access to effective remedy for human rights abuses linked to the impacts of technology companies, wherever the harms occur, including harms resulting from the operations of their subsidiaries (whether foreign or domestic). Redress mechanisms should be made easily accessible and understandable to enable individuals to file complaints when their rights have been infringed.

ANNEX 1. TIKTOK PRIVACY POLICIES COMPARISON

TIKTOK WHAT INFORMATION WE COLLECT

Table 1: Information You Provide

	EU/UK/Switzerland	US	Other regions
Profile information	We collect information that you provide when you set up an account, such as your date of birth, username, email address and/or telephone number, and password. You can add other information to your profile, such as a bio or a profile photo.	Account and profile information, such as name, age, username, password, language, email, phone number, social media account information, and profile image.	You give us information when you register on the Platform, including your username, password, date of birth (where applicable), email address and/or telephone number, information you disclose in your user profile, and your photograph or profile video.
User Content	We collect the content you create or publish through the Platform, such as photographs, videos, audio recordings, livestreams, comments, hashtags, feedback, reviews, and the associated metadata (such as when, where, and by whom the content was created). Even if you are not a user, information about you may appear in content created or published by users on the Platform. We collect User Content through pre-loading at the time of creation, import, or upload, regardless of whether you choose to save or upload that User Content, for example, to recommend music based on the video. We also collect content (such as text, images, and video) from your device's clipboard if you choose to copy and paste content to or from the Platform or share content between it and a third party platform. In addition, we collect location information (such as tourist attractions, shops, or other points of interest) if you choose to add the location information to your User Content.	User-generated content, including comments, photographs, livestreams, audio recordings, videos, text, hashtags, and virtual item videos that you choose to create with or upload to the Platform ("User Content") and the associated metadata, such as when, where, and by whom the content was created. Even if you are not a user, information about you may appear in User Content created or published by users on the Platform. When you create User Content, we may upload or import it to the Platform before you save or post the User Content (also known as pre-uploading), for example, in order to recommend audio options, generate captions, and provide other personalized recommendations. If you apply an effect to your User Content, we may collect a version of your User Content that does not include the effect.	We process the content you generate on the Platform, including photographs, audios and videos you upload or create, comments, hashtags, feedback, reviews, and livestreams you make, and the associated metadata, such as when, where, and by whom the content was created ("User Content"). Even if you are not a user, information about you may appear in User Content created or published by users on the Platform. We collect User Content through pre-loading at the time of creation, import, or upload, regardless of whether you choose to save or upload that User Content, in order to recommend audio options and provide other personalized recommendations. If you apply an effect to your User Content, we may collect a version of your User Content that does not include the effect.
Direct Messages	If you communicate with others using direct messages, we collect the content of the message and the associated metadata (such as the time the message was sent, received and/or read, as well as the participants in the communication). We also collect the messages you send or receive through our chat functionality when communicating with merchants who sell goods to you, and your use of virtual assistants when purchasing items through the Platform. We do this to block spam, detect crime, and to safeguard our users.	Messages, which include information you provide when you compose, send, or receive messages through the Platform's messaging functionalities. They include messages you send through our chat functionality when communicating with merchants who sell goods to you, and your use of virtual assistants when purchasing items through the Platform. That information includes the content of the message and information about the message, such as when it was sent, received, or read, and message participants. Please be aware that messages you choose to send to other users of the Platform will be accessible by those users and that we are not responsible for the manner in which those users use or share the messages.	We collect information you provide when you compose, send, or receive messages through the Platform's messaging functionalities. They include messages you send or receive through our chat functionality when communicating with merchants who sell goods to you, and your use of virtual assistants when purchasing items through the Platform. That information includes the content of the message and information about the message, such as when it was sent, received, or read, and message participants. Please be aware that messages you choose to send to other users of the Platform will be accessible by those users and that we are not responsible for the manner in which those users use or share the messages.
Clipboard		Information, including text, images, and videos, found in your device's clipboard, with your permission. For example, if you choose to initiate information sharing with a third-party platform, or choose to paste content from the clipboard onto the Platform, we access this information stored in your clipboard in order to fulfill your request.	We may access content, including text, images, and video, found in your device's **clipboard**, with your permission. For example, if you choose to initiate content sharing with a third-party platform, or choose to paste content from the clipboard into the Platform, we access this information stored in your clipboard in order to fulfill your request.

Your Contacts	If you choose to sync your contacts, we will collect information from your device's phone book such as names, phone numbers, and email addresses, and match that information to users of the Platform. If you choose to find other users through your social network contacts, we will collect your public profile information as well as names and profiles of your social network contacts		
Your phone and social network contacts		Your phone and social network contacts, with your permission. If you choose to find other users through your phone contacts, we will access and collect information such as names, phone numbers, and email addresses, and match that information against existing users of the Platform. If you choose to find other users through your social network contacts, we will collect your public profile information as well as names and profiles of your social network contacts.	If you choose to sync your phone contacts, we will access and collect information such as names, phone numbers, and email addresses, and match that information against existing users of the Platform. If you choose to share your social network contacts, we will collect your public profile information as well as names and profiles of your social network contacts.
Purchase Information	When you make a purchase or payment on or through the Platform, including when you buy TikTok Coins or purchase goods through our shopping features, we collect information about the purchase or payment transaction, such as payment card information, billing, delivery, and contact information, and items you purchased.	Purchase information, including payment card numbers or other third-party payment information (such as PayPal) where required for the purpose of payment, and billing and shipping address. We also collect information that is required for extended warranty purposes and your transaction and purchase history on or through the Platform.	When you make a purchase or payment on or through the Platform, including when you buy TikTok Coins or purchase goods through our shopping features, we collect information about the purchase or payment transaction, such as payment card information, billing, delivery, and contact information, and items you purchased.
Surveys, Research, and Promotions	We collect information you provide if you choose to participate in a survey, research, promotion, contest, marketing campaign, or event conducted or sponsored by us.	Information you share through surveys or your participation in challenges, research, promotions, marketing campaigns, events, or contests such as your gender, age, likeness, and preferences.	Information through surveys, research, promotion, contests, marketing campaigns, challenges, competitions or events conducted or sponsored by us, in which you participate.
Information When You Contact Us	When you contact us, we collect the information you send us, such as proof of identity or age, feedback or inquiries about your use of the Platform or information about possible violations of our Terms of Service (our "**Terms**"), Community **Guidelines** (our "Guidelines"), or other policies.	Your choices and communication preferences. Information in correspondence you send to us, including when you contact us for support.	Information in **correspondence** you send to us, including when you contact us for support or feedback.
Proof of your identity or age		Information to verify an account such as proof of identity or age.	We sometimes ask you to provide proof of identity or age in order to use certain features, such as livestream or verified accounts, or when you apply for a Pro Account, ensure that you are old enough to use the Platform, or in other instances where verification may be required.

Table 2: Automatically Collected Information

	EU/UK/Switzerland	US	Other regions
Usage Information	We collect information about how you engage with the Platform, including information about the content you view, the duration and frequency of your use, your engagement with other users, your search history and your settings.	We collect information regarding your use of the Platform and any other User Content that you generate through or upload to our Platform.	We collect information regarding your use of the Platform, e.g., how you engage with the Platform, including how you interact with content we show to you, the advertisements you view, videos you watch and problems encountered, browsing and search history, the content you like, the content you save to 'My Favourites', the users you follow and how you engage with mutual followers.
Device Information		We collect certain information about the device you use to access the Platform, such as your IP address, user agent, mobile carrier, time zone settings, identifiers for advertising purposes, model of your device, the device system, network type, device IDs, your screen resolution and operating system, app and file names and types, keystroke patterns or rhythms, battery state, audio settings and connected audio devices. We automatically assign you a device ID and user ID. Where you log-in from multiple devices, we will be able to use information such as your device ID and user ID to identify your activity across devices. We may also associate you with information collected from devices other than those you use to log-in to the Platform.	
Inferred Information	We infer your attributes (such as age-range and gender) and interests based on the information we have about you. We use inferences, for example, to keep the Platform safe, for content moderation and, where permitted, to serve you personalised ads based on your interests.		We also infer your attributes, including your interests, gender and age range for the purpose of personalising content.
Technical Information we collect about you	We collect certain device and network connection information when you access the Platform. This information includes your device model, operating system, keystroke patterns or rhythms, IP address, and system language. We also collect service-related, diagnostic, and performance information, including crash reports and performance logs. We automatically assign you a device ID and user ID. Where you log-in from multiple devices, we use information such as your device ID and user ID to identify your activity across devices to give you a seamless log-in experience and for security purposes.		We collect certain information about the device you use to access the Platform, such as your IP address, user agent, mobile carrier, time zone settings, identifiers for advertising purposes, model of your device, the device system, network type, device IDs, your screen resolution and operating system, app and file names and types, keystroke patterns or rhythms, battery state, audio settings and connected audio devices. Where you log-in from multiple devices, we will be able to use your profile information to identify your activity across devices. We may also associate you with information collected from devices other than those you use to log-in to the Platform.
Location Information	We automatically collect information about your approximate location (e.g. country, state, or city) based on your Technical Information (such as SIM card and IP address). Also, where you enable location services for the TikTok app within your device settings, we collect approximate location information from your device. Click here to learn more about how we collect Location Information.	We collect information about your approximate location, including location information based on your SIM card and/or IP address. In addition, we collect location information (such as tourist attractions, shops, or other points of interest) if you choose to add the location information to your User Content. Current versions of the app do not collect precise or approximate GPS information from U.S. users. If you are still using an older version that allowed for collection of precise or approximate GPS information (last release in August 2020) and you granted us permission to do so, we may collect such information.	We collect information about your approximate location, including location information based on your SIM card and/or IP address. With your permission, we may also collect precise location data (such as GPS). In addition, we collect location information (such as tourist attractions, shops, or other points of interest) if you choose to add location information to your User Content.

Image and Audio Information		We may collect information about the videos, images and audio that are a part of your User Content, such as identifying the objects and scenery that appear, the existence and location within an image of face and body features and attributes, the nature of the audio, and the text of the words spoken in your User Content. We may collect this information to enable special video effects, for content moderation, for demographic classification, for content and ad recommendations, and for other non-personally-identifying operations. We may collect biometric identifiers and biometric information as defined under U.S. laws, such as faceprints and voiceprints, from your User Content. Where required by law, we will seek any required permissions from you prior to any such collection. Click here to learn more.	We may collect information about the videos, images and audio that are a part of your User Content, such as identifying the objects and scenery that appear, the existence and location within an image of face and body features and attributes, the nature of the audio, and the text of the words spoken in your User Content. We may collect this information to enable special video effects, for content moderation, for demographic classification, for content and ad recommendations, and for other non-personally-identifying operations.
Content Characteristics and Features	We detect and collect characteristics and features about the videos, images, and audio recordings that are part of your User Content, for example, by identifying objects and scenery, the existence or location within an image of a face or other body parts; and the text of words spoken in your User Content. We do this, for example, for content moderation and to provide special effects (such as video filters and avatars) and captions.		
Metadata		When you upload or create User Content, you automatically upload certain metadata that is connected to the User Content. Metadata describes other data and provides information about your User Content that will not always be evident to the viewer. For example, in connection with your User Content the metadata can describe how, when, where, and by whom the piece of User Content was created, collected, or modified and how that content is formatted. It also includes information, such as your account name, that enables other users to trace back the User Content to your user account. Additionally, metadata includes data that you choose to provide with your User Content, e.g., any hashtags used to mark keywords to the video and captions.	

Table 3: Information From Other Sources

	EU/UK/Switzerland	US	Other regions
Advertising, Measurement and Other Partners	Advertisers, measurement and other partners share information with us about you and the actions you have taken outside of the Platform, such as your activities on other websites and apps or in stores, including the products or services you purchased, online or in person. These partners also share information with us, such as mobile identifiers for advertising, hashed email addresses and phone numbers, and cookie identifiers, which we use to help match you and your actions outside of the Platform with your TikTok account. Some of our advertisers and other partners enable us to collect similar information directly from their website or app by integrating our TikTok Advertiser Tools (such as TikTok Pixel).	Advertisers, measurement and other partners share information with us about you and the actions you have taken outside of the Platform, such as your activities on other websites and apps or in stores, including the products or services you purchased, online or in person. These partners also share information with us, such as mobile identifiers for advertising, hashed email addresses and phone numbers, and cookie identifiers, which we use to help match you and your actions outside of the Platform with your TikTok account. Some of our advertisers and other partners enable us to collect similar information directly from their websites or apps by integrating our TikTok Advertiser Tools (such as TikTok Pixel).	Advertisers, measurement and other partners share information with us about you and the actions you have taken outside of the Platform, such as your activities on other websites and apps or in stores, including the products or services you purchased, online or in person. These partners also share information with us, such as mobile identifiers for advertising, hashed email addresses and phone numbers, and cookie identifiers, which we use to help match you and your actions outside of the Platform with your TikTok account. Some of our advertisers and other partners enable us to collect similar information directly from their websites or apps by integrating our TikTok Advertiser Tools (such as TikTok Pixel).
Merchants, Payment and Transaction Fulfillment Providers	We receive information about you from merchants as well as payment and transaction fulfillment providers, such as payment confirmation details, and information about the delivery of products you have purchased through our shopping features.		We may receive information from merchants and payment and transaction fulfillment providers about you, such as payment confirmation details, and information about the delivery of products you have purchased through our shopping features.
Third Party Platforms and Partners	Third party platforms provide us with information (such as your email address, user ID, and public profile) when you choose to sign up for or log in to the Platform using sign-in features provided by those third parties. We may also receive contact information that you hold or is held about you when contact information is synced with our Platform by you or another user. When you interact with any third party service (such as third party apps, websites or products) that integrate TikTok Developer Tools, we will receive the information necessary to provide you with features like cross-service authentication or cross-posting. For example, this will happen if you log in to another platform with your TikTok account or if you use TikTok's "share" button on a third party platform to share content from there to the Platform.	If you choose to sign-up or log-in to the Platform using a third-party service such as Facebook, Twitter, Instagram, or Google, or link your TikTok account to a third-party service, we may collect information from the service– for example, your public profile information (such as nickname), email, and contact list.	If you choose to register or use the Platform using a third-party social network account details (e.g., Facebook, Twitter, Instagram, Google) or login service, you will provide us or allow to provide us with your username, public profile, and other possible information related to such account. We will likewise share certain information with your social network such as your app ID, access token and the referring URL. If you link your TikTok account to another service, we may receive information about your use of that service.
Others	We may receive information about you from others, for example, where you are included or mentioned in User Content, Direct Messages, in a complaint, appeal, request or feedback submitted by a user or third party, or if your contact information is provided to us by a user.	We may receive information about you from others, including where you are included or mentioned in User Content, direct messages, in a complaint, appeal, request or feedback submitted to us, or if your contact information is provided to us. We may collect information about you from other publicly available sources. We may obtain information about you from certain affiliated entities within our corporate group, including about your activities on their platform.	We may receive information about you from others, including where you are included or mentioned in User Content, direct messages, in a complaint, appeal, request or feedback submitted to us, or if your contact information is provided to us. We may collect information about you from other publicly available sources. We may obtain information about you from certain affiliated entities within our corporate group, including about your activities on their platforms.

Table 4: How We Use Your Information

EU/UK/Switzerland	US	Other regions
Provide and administer the Platform, such as enabling you to create, share, and consume content, to interact with other users and their content, and provide user support.	To fulfill requests for products, services, Platform functionality, support and information for internal operations, including troubleshooting, data analysis, testing, research, statistical, and survey purposes and to solicit your feedback.	To fulfill requests for products, services, Platform functionality, support and information for internal operations, including troubleshooting, data analysis, testing, research, statistical, and survey purposes and to solicit your feedback.
Provide our shopping features and facilitate the purchase and delivery of products, goods and services, including sharing your information with merchants, payment and transaction fulfilment providers, and other service providers in order to process your orders.	To customize the content you see when you use the Platform. For example, we may provide you with services based on the country settings you have chosen or show you content that is similar to content that you have liked or interacted with.	To provide our shopping features and facilitate the purchase and delivery of products, goods and services, including sharing your information with merchants, payment and transaction fulfillment providers, and other service providers in order to process your orders.
Personalise and customise your experience on the Platform, such as providing your 'For You' feed.	To send promotional materials from us or on behalf of our affiliates and trusted third parties.	To personalise the content you see when you use the Platform. For example, we may provide you with services based on the country settings you have chosen or show you content that is similar to content that you have liked or interacted with.
Enforce our Terms, Guidelines, and other policies that apply to you. We review User Content and other information to protect the safety and well-being of our community.	To improve and develop our Platform and conduct product development.	To send promotional materials, including by instant messaging or email, from us or on behalf of our affiliates and trusted third parties.
Provide certain interactive features, such as enabling your content to be used in other users' videos, and to suggest your account to other users to help connect you with other users.	To measure and understand the effectiveness of the advertisements we serve to you and others and to deliver advertising, including targeted advertising, to you on the Platform.	To improve and develop our Platform and conduct product development.
Provide and improve our advertising services, including to serve ads (including personalised ads, where permitted) and to measure and understand the effectiveness of the ads and other content.	To make suggestions and provide a customized ad experience.	To measure and understand the effectiveness of the advertisements and other content we serve to you and others, and to deliver advertising, including targeted advertising, to you on the Platform.
Maintain and enhance the safety, security, and stability of the Platform by identifying and addressing technical or security issues or problems (such as technical bugs, spam accounts, and detecting abuse, fraud, and illegal activity).	To support the social functions of the Platform, including to permit you and others to connect with each other (for example, through our Find Friends function), to suggest accounts to you and others, and for you and others to share, download, and otherwise interact with User Content posted through the Platform.	To support the social functions of the Platform, including to permit you and others to connect with each other (for example, through our Find Friends function) and to share whether you are active on the Platform (and other information which you choose to share) with your friends, to provide our messaging service if you choose to use this function, to suggest accounts to you and others, and for you and others to share, download, and otherwise interact with User Content posted through the Platform.
Review, improve, and develop the Platform, including by monitoring interactions and usage across your devices, analysing how people are using it, and by training and improving our technology, such as our machine learning models and algorithms.	To use User Content as part of our advertising and marketing campaigns to promote the Platform.	To enable you to participate in the virtual items program.
Share your information with third party platforms to provide you with features, like content sharing at your request when you integrate your TikTok account with a third party service.	To understand how you use the Platform, including across your devices.	To allow you to participate in interactive features of the Platform, such as enabling your content to be used in other users' videos.

Facilitate research conducted by independent researchers that meets certain criteria.	To infer additional information about you, such as your age, gender, and interests.	To use User Content as part of our advertising and marketing campaigns to promote the Platform, to invite you to participate in an event, and to promote popular topics, hashtags and campaigns on the Platform.
Promote the Platform or third party services through marketing communications, contests, or promotions.	To help us detect abuse, fraud, and illegal activity on the Platform.	To understand how you use the Platform, including across your devices.
Comply with our legal obligations, or as necessary to perform tasks in the public interest, or to protect the vital interests of our users and other people.	To promote the safety and security of the Platform, including by scanning, analyzing, and reviewing User Content, messages and associated metadata for violations of our Terms of Service, Community Guidelines, or other conditions and policies.	To infer additional information about you, such as your age range, gender, and interests.
	To verify your identity in order to use certain features, such as livestream or verified accounts, or when you apply for a Pro Account, to ensure that you are old enough to use the Platform (as required by law), or in other instances where verification may be required.	To help us detect and combat abuse, harmful activity, fraud, spam, and illegal activity on the Platform.
	To communicate with you, including to notify you about changes in our services.	To ensure content is presented in the most effective manner for you and your device.
	To announce you as a winner of our contests or promotions if permitted by the promotion rule, and to send you any applicable prizes.	To promote the safety, security of the Platform, including by scanning, analyzing, and reviewing User Content, messages and associated metadata for violations of our Terms of Service, Community Guidelines, or other conditions and policies.
	To enforce our Terms of Service, Community Guidelines, and other conditions and policies.	To facilitate research conducted by independent researchers that meets certain criteria.
	Consistent with your permissions, to provide you with location-based services, such as advertising and other personalized content.	To verify your identity or age.
	To train and improve our technology, such as our machine learning models and algorithms.	To communicate with you, including to notify you about changes in our services.
	To combine all the Information We Collect or receive about you for any of the foregoing purposes.	To announce you as a winner of our contests or promotions if permitted by the promotion rule, and to send you any applicable prizes.
	To facilitate sales, promotion, and purchases of goods and services and to provide user support.	To enforce our Terms of Service, Community Guidelines, and other conditions and policies.
	For any other purposes disclosed to you at the time we collect your information or pursuant to your consent.	Consistent with your permissions, to provide you with location-based services, such as advertising and other personalized content.
		To train and improve our technology, such as our machine learning models and algorithms.
		To facilitate and fulfill sales, promotion, and purchases of goods and services and to provide user support.

Table 5: How We Share Your Information

EU/UK/Switzerland	US	Other regions
	We are committed to maintaining your trust, and while TikTok does not sell your personal information or share your personal information with third parties for purposes of cross-context behavioral advertising where restricted by applicable law, we want you to understand when and with whom we may share the Information We Collect for business purposes.	We share your information with the following parties:
Service Providers We engage service providers that help us provide, support, and develop the Platform and understand how it is used. They provide services such as: cloud hosting, content delivery, customer and technical support, content moderation, marketing, analytics, and online payments. We share Information You Provide, Automatically Collected Information, and Information From Other Sources with these service providers as necessary to enable them to provide their services.	**Service Providers and Partners** We share the categories of personal information listed above with service providers and business partners to help us perform business operations and for business purposes, including research, payment processing and transaction fulfillment, database maintenance, administering contests and special offers, technology services, deliveries, sending communications, advertising and marketing services, analytics, measurement, data storage and hosting, disaster recovery, search engine optimization, and data processing. These service providers and business partners may include: • Payment processors and transaction fulfillment providers, who may receive the Information You Provide, Information From Other Sources, and Automatically Collected Information but who do not receive your message data, including, in particular, the following third-party payment providers/processors: PayPal (https://www.paypal.com/us/webapps/mpp/ua/privacy-full) and Stripe (https://stripe.com/en-ie/privacy). • Customer and technical support providers, who may receive the Information You Provide, Information From Other Sources, and Automatically Collected Information. • Researchers who may receive the Information You Provide, Information From Other Sources, and Automatically Collected Information but would not receive your payment information or message data. • Advertising, marketing, and analytics vendors, who may receive the Information You Provide, Information From Other Sources, and Automatically Collected Information but would not receive your payment information or message data.	**Business Partners** If you choose to register to use the Platform using your social network account details (e.g., Facebook, Twitter, Instagram, Google), you will provide us or allow your social network to provide us with your phone number, email address, username and public profile. We will likewise share certain information with the relevant social network such as your app ID, access token and the referring URL. If you choose to allow a third-party service to access your account, we will share certain information about you with the third party. Depending on the permissions you grant, the third party may be able to obtain your account information and other information you choose to provide. Where you opt to share content on social media platforms, the video, username and accompanying text will be shared on that platform or, in the case of sharing via instant messaging platforms such as Whatsapp, a link to the content will be shared.

Partners		
Third Party Platforms and Partners We share limited information which may include Information You Provide, Technical Information, and Usage Information with third party platforms and partners whose platform or services are integrated with the Platform. We do this to give you a seamless experience, allow your content to be shared on other platforms, and/or enable third party platforms and partners to better authenticate users. Some examples include if you: • log-in to a third party platform using your account, we will share your basic account information and any other Information You Provide, • sign-up or log-in to the Platform using your account details from a third party platform (such as Facebook or Google), we will share certain Technical Information to facilitate this, - share User Content you publish on the Platform on other social media platforms, we will share your User Content and related information.		**Service Providers** We provide information and content to service providers who support our business, such as cloud service providers and providers of content moderation services to ensure that the Platform is a safe and enjoyable place and service providers that assist us in marketing the Platform. **Payment processors and transaction fulfillment providers:** If you choose to buy Coins or conduct other payment related transactions, we will share data with the relevant payment provider to facilitate this transaction. For Coin transactions, we share a transaction ID to enable us to identify you and credit your account with the correct value in coins once you have made the payment. **Analytics providers:** We use analytics providers to help us in the optimisation and improvement of the Platform. Our third-party analytics providers also help us serve targeted advertisements.
Advertisers We provide advertisers with aggregate information about the performance of their ads and other content on the Platform in order to help them measure their effectiveness. We create this aggregate information using Information You Provide, Automatically Collected Information, and Information From Other Sources. We share your information directly with advertisers where you give us your permission.	Advertising, marketing, and analytics vendors, who may receive the Information You Provide, Information From Other Sources, and Automatically Collected Information but would not receive your payment information or message data.	**Advertisers, Advertising Networks and Measurement Partners** We share information with advertisers and third-party measurement companies to show how many and which users of the Platform have viewed or clicked on an advertisement. If you use the TikTok Lite version of TikTok, we share information with advertising networks to display personalised advertisements to you on the TikTok Lite app and elsewhere online. We are not responsible for the privacy practices of these third parties, and the information practices of these third parties are not covered by this Privacy Policy.
Measurement and Data Partners We also share Information You Provide, Technical Information and Usage Information with third party measurement providers who help us measure advertising served on the Platform and help our advertisers determine how effective their ads have been.		
Merchants, Payment and Transaction Fulfilment Providers, and Other Service Providers When you make a purchase through the shopping features on our Platform, we share Purchase Information related to the transaction with the merchant, payment and transaction fulfilment providers, and other service providers. For example, we will share the order items, contact details and delivery information so your order can be processed. We may also share certain Technical Information about your device or connection with these parties to help ensure the security of the transaction.	Payment processors and transaction fulfillment providers, who may receive the Information You Provide, Information From Other Sources, and Automatically Collected Information but who do not receive your message data, including, in particular, the following third-party payment providers/processors: PayPal (https://www.paypal.com/us/webapps/mpp/ua/privacy-full) and Stripe (https://stripe.com/en-ie/privacy).	

Our Corporate Group As a global company, the Platform is supported by certain entities within our corporate group ("**Corporate Group**"). These entities process Information You Provide, Automatically Collected Information, and Information From Other Sources for us, as necessary to provide certain functions, such as storage, content delivery, security, research and development, analytics, online payments, customer and technical support, and content moderation. See Our Global Operations and Data Transfers for additional information.	**Within Our Corporate Group** As a global company, the Platform is supported by certain entities within our corporate group, which are given limited remote access to Information We Collect as necessary to enable them to provide certain important functions. To learn more about how we share information with certain corporate group entities, see here.	
Others We share your information in other limited scenarios as follows: **Users and the Public** Based on your privacy settings, your information, including your Profile Information, User Content, and Usage Information may be visible to other users and the public. For example, if you have a public account and have not restricted the visibility of your posts individually, your Profile Information and User Content can be viewed or shared by anyone on or off the Platform, whether or not they have a TikTok account. Depending on your privacy settings, your Profile Information and User Content may also appear on search engines, content aggregators, and news sites. You can learn about account types and privacy settings, including how to limit the audience for your videos here.	**In Connection with a Sale, Merger, or Other Business Transfer** We may share all of the Information We Collect in connection with a substantial corporate transaction, such as the sale of a website, a merger, consolidation, asset sales, or in the unlikely event of bankruptcy.	
Users of Our Analytics Services We provide aggregated statistics and insights to help people and businesses understand how people are engaging with the Platform. For example, creators and advertisers can receive information about the number of views, likes, comments and shares of their videos, as well as aggregate demographic information about their followers and the viewers of their videos. We create this aggregate information using Information You Provide and Automatically Collected Information.		
Independent Researchers We share your information with independent researchers to facilitate research that meets certain criteria as described in Our Legal Bases and How We Process Your Information.	Researchers who may receive the Information You Provide, Information From Other Sources, and Automatically Collected Information but would not receive your payment information or message data.	**Independent Researchers** We share your information with independent researchers to facilitate research that meets certain criteria.
Corporate Transactions Your information may be disclosed to third parties in connection with a corporate transaction, such as a merger, sale of assets or shares, reorganisation, financing, change of control, or acquisition of all or a portion of our business.		**Our Corporate Group** We may also share your information with other members, subsidiaries, or affiliates of our corporate group, including to provide the Platform, to improve and optimise the Platform, to prevent illegal use and to support users.

Legal Obligations and Rights

We may access, preserve, and share the information described in "What Information We Collect" with law enforcement agencies, public authorities, researchers, copyright holders, or other third parties if we have good faith belief that it is necessary to:

- comply with applicable law, legal process or government requests, as consistent with internationally recognised standards,
- protect the rights, property, and safety of our users, copyright holders, and others, including to protect life or prevent imminent bodily harm. For example, we may provide information (such as your IP address) to law enforcement in the event of an emergency where someone's life or safety is at risk,
- investigate potential violations of and enforce our Terms, Guidelines, or any other applicable terms, policies, or standards, or
- detect, investigate, prevent, or address misleading activity, copyright infringement, or other illegal activity.

To learn more about how we handle requests from law enforcement agencies and public authorities, see our Law Enforcement Guidelines.

For Legal Reasons

We may disclose any of the Information We Collect to respond to subpoenas, court orders, legal process, law enforcement requests, legal claims, or government inquiries, and to protect and defend the rights, interests, safety, and security of the Platform, our affiliates, users, or the public. We may also share any of the Information We Collect to enforce any terms applicable to the Platform, to exercise or defend any legal claims, and comply with any applicable law.

For Legal Reasonss

We will share your information with law enforcement agencies, public authorities or other organisations if legally required to do so, or if such use is reasonably necessary to:

- comply with legal obligation, process or request;
- enforce our Terms of Service and other agreements, policies, and standards, including investigation of any potential violation thereof;
- detect, prevent or otherwise address security, fraud or technical issues; or
- protect the rights, property or safety of us, our users, a third party or the public as required or permitted by law (including exchanging information with other companies and organisations for the purposes of fraud protection and credit risk reduction).

With Your Consent

We may share your information for other purposes pursuant to your consent or at your direction.

We partner with third-party services (such as Facebook, Instagram, Twitter, and Google) to offer you a seamless sign-up, log-in, and content-sharing experience. We may share information about you with these third-party services if you choose to use these features. For example, the services may receive information about your activity on the Platform and may notify your connections on the third-party services about your use of the Platform, in accordance with their privacy policies. If you choose to allow a third-party service to access your account, we will share certain information about you with the third party. Depending on the permissions you grant, the third party may be able to obtain your account information and other information you choose to provide.

If you choose to engage in public activities on the Platform, you should be aware that any information you share may be read, collected, or used by other users. You should use caution in disclosing personal information while using the Platform. We are not responsible for the information you choose to submit.

When you make a purchase from a third party on the Platform, including from a merchant selling products through our shopping features, we share the information related to the transaction with that third party and their service providers and transaction fulfillment providers. By making the purchase, you are directing us to share your information in this way. These entities may use the information shared in accordance with their privacy policies.

Public Profiles

Please note that if your profile is public, your content will be visible to anyone on the Platform and may also be accessed or shared by your friends and followers as well as third parties such as search engines, content aggregators and news sites. You can change who can see a video each time you upload a video. Alternatively, you can change your profile to default private by changing your settings to 'Private Account' in "Manage my account" settings.

			Sale, Merger or Other Business Transactions We may also disclose your information to third parties: • in the event that we sell or buy any business or assets (whether a result of liquidation, bankruptcy or otherwise), in which case we will disclose your data to the prospective seller or buyer of such business or assets; or • if we sell, buy, merge, are acquired by, or partner with other companies or businesses, or sell some or all of our assets. In such transactions, user information may be among the transferred assets.
			Merchants, Payment and Transaction Fulfillment Providers, and Other Service Providers When you make a purchase through our shopping features, we share the information related to the transaction with the merchant, payment and transaction fulfillment providers, and other service providers. For example, we will share the order items, contact details and delivery information so your order can be processed. These entities may use the information shared in accordance with their privacy policies.

ANNEX 2. TIKTOK'S WRITTEN RESPONSE OF 12 JULY 2023

TikTok response page 1

TikTok

July 12th, 2023

Dear Ms. Abdul Rahim,

Thank you once again for the outreach and for continuing the conversation started earlier this spring with the team at Amnesty Tech. We appreciate the time you've taken to develop this questionnaire related to children's rights in the digital environment and have collected and consolidated responses to the items highlighted in your letter. To that end, we would like to share more about TikTok's efforts across each of the areas highlighted in the questionnaire:

DUE DILIGENCE

Our approach to youth safety is informed by our larger commitment to human rights, including the United Nations Guiding Principles on Business and Human Rights and its call to conduct human rights due diligence. Our teams, which are composed of youth safety policy experts, proactively assess human rights risks related to young people. We also work to embed a human rights-based approach across all our Community Guidelines. We have Global Advisory Councils, which include experts in children's rights and we are members of the WeProtect Global Alliance and the Tech Coalition where we engage with our peers on current and upcoming risks. Furthermore, our recently announced Youth Council will serve as an additional sounding board to create policies, products, and programs in tune with the needs of our users. We also work with industry experts, non-governmental organizations, and industry associations around the world in our commitment to building a safe platform for our community. We collaborate with organizations in different regions to share best practices, create programs, and exchange ideas on safety-related topics. We regularly consult with external stakeholders and partners in this area and will continue to update you on our work in future.

We believe that human rights are integral to the work of all teams at TikTok. At TikTok, thousands of people are focused on helping to make our platform safe for our community to explore entertaining content and share their creativity. We have a centralized team that manages our efforts across the company, and we have champions across the organization, empowered by leadership to address any identified risks. TikTok's policies on youth safety and well-being, as articulated in this sub-section in the Community Guidelines, are developed by our Trust & Safety Product Policy team, and are overseen by a sub-team that specializes in youth safety and well-being issues. This sub-team closely collaborates with the Product Policy team responsible for account-level enforcement. The Platform Fairness team specializes in issues of human rights, fairness, and inclusion and applies a multifaceted approach to the review and revision of policies, product features, and algorithmic systems. In the future, we will conduct periodic impact assessments in partnership with third parties, which may take the form of company-wide assessments, team assessments, and product or business line specific assessments. In our human rights risk assessment process, gender is one of many considerations that has been identified to

have an impact on the risk level, and we design our mitigation measures to address such considerations.

TikTok embeds safety-by-design principles, which means that we implement a safety-first approach in the design of the platform and that user safety is embedded as a priority throughout the product and feature development decision-making processes. TikTok's goal is to provide young people with an experience that is developmentally appropriate and helps to ensure a safe space for self-exploration. TikTok is only for those aged at least 13, or 14 in certain jurisdictions. In the US, we offer a curated, view-only experience for those under age 13 that includes additional safeguards and privacy protections. We work to design tools and policies that promote a safe and age-appropriate experience for teens 13-17. In relation to product design, we take several steps including: (1) limiting access to certain product features, (2) utilizing Content Levels that sort content by levels of thematic comfort, (3) using restrictive default privacy settings, and (4) making content uploaded by accounts registered to users under 16 ineligible for the For You Feed (FYF).

Our policies prohibit content that may put young people at risk of exploitation, or psychological, physical, or developmental harm. We have many policies to promote youth safety on the platform. Below are the risks we have identified, and what is appropriate/inappropriate for our teen users.

NOT allowed

- Sexual exploitation of young people, including child sexual abuse material (CSAM), grooming, solicitation, and pedophilia
- Physical abuse, neglect, endangerment, and psychological abuse of young people
- Trafficking of young people, promotion or facilitation of underage marriage, and recruitment of child soldiers
- Sexual activity of young people
- Nudity or significant body exposure of young people
- Allusions to sexual activity by young people
- Seductive performances by young people
- Consumption of alcohol, tobacco products, and drugs by young people

Age-restricted (18 years and older)

- Cosmetic surgery that does not include risk warnings, including before-and-after images, videos of surgical procedures, and messages discussing elective cosmetic surgery
- Activities that are likely to be imitated and may lead to any physical harm
- Significant body exposure of adults
- Seductive performances by adults
- Sexualized posing by adults
- Allusions to sexual activity by adults
- Blood of humans and animals
- Consumption of excessive amounts of alcohol by adults
- Consumption of tobacco products by adults

For You Feed ineligible

- Any content created by an under-16 account
- Moderate body exposure of young people
- Intimate kissing or sexualized posing by young people

If we become aware of youth exploitation on our platform, we will ban the account, as well as any other accounts belonging to the person, and make reports to law enforcement/NCMEC as necessary.

We also offer several tools and controls to support our community's safety and well-being, such as the guides within our Safety Center, which focus on our approach to safety, privacy and security on TikTok. To specifically support our younger community on TikTok, we have developed a Youth Portal, which offers both in-app tools and educational content for our younger users to enjoy their best possible experience.

DATA COLLECTION

Our privacy policies set out, among other things, what data we collected as well as how we use or share such data from TikTok users. Please also refer to this article in our help center for information about our recommendation system. TikTok does not use "sensitive personal data," as the term is defined under GDPR, to personalize content. Nor does TikTok use data collected from users and machine learning to draw inferences about protected characteristics beyond gender and age-range. TikTok does not sell user's personal information or share user's personal information with third parties for purposes of cross-context behavioral advertising where restricted by applicable law.

At TikTok, we take special care when crafting the experiences teens have on the platform, including the ads they see. Currently, some teens may be shown ads based on their activities on and off TikTok, such as the accounts they follow, the videos they like, and their profile information. On June 28, 2023, we announced that we are restricting the types of data that can be used to show ads to teens by region. This means that people in the United States aged 13 to 15 will no longer see personalized ads on TikTok based on their activities off TikTok and people in the European Economic Area, United Kingdom, and Switzerland aged 13 to 17 will no longer see personalized ads on TikTok based on their activities on or off TikTok. We're continuing to work toward providing all people on TikTok with transparency and controls so they can choose the experience that's right for them.

TikTok's Anti-Discrimination Ad Policy prohibits advertisers from using our ads products to discriminate against people unlawfully. Accordingly, advertisers may not include any unlawfully discriminatory or harassing content in their advertising or any content that encourages unlawful discrimination or harassment. In addition, advertisers may not use audience selection tools to: (a) wrongfully target specific groups of people for advertising in a way that breaches applicable laws or regulations; or (b) wrongfully exclude specific groups of people from seeing their ads, in breach of applicable laws or regulations.

In order to prioritize our users and ensure a positive experience on our platform, we do not allow advertisers to unlawfully target or exclude users based on the following categories, including without limitation by using Custom Audiences or the tools and audiences made available on our platform:

Categories advertisers may not use for discriminatory ad targeting where unlawful:

- Legally protected classes based on the local laws of the region, such as race, ethnicity, age, familial status, and sexual orientation
- National identity, country of citizenship, country of origin, or veteran status or identity or beliefs in regards to political groups, religion or union affiliations
- Personal, financial, or legal hardships
- Individual health statuses or disabilities, including mental, physical, genetic, or emotional health and conditions

When advertisers use TikTok's advertiser tools (e.g., to display advertisements on their own websites and applications), TikTok prohibits those advertisers from transmitting certain types of sensitive information back to TikTok. Section 2.8 of TikTok's Business Products (Data) Terms prohibits advertisers from sharing with, or enabling TikTok to collect, "Business Products Data that you know or ought reasonably to know is from or about children or that includes health or financial information, or other categories of sensitive information (including any information defined as sensitive or special category data under applicable laws, regulations and applicable industry guidelines. TikTok restricts advertisers' use of lookalike audiences based on its Anti-Discrimination Ad Policy (referenced above) and we have policies that restrict specific ad categories to 18+.

AGE GATE AND MINIMUM AGE APPEALS

TikTok has a 12+ rating in the App Store, which lets parents use device-level controls to block people under the age of 12 from downloading the app. To help keep people from using TikTok if they're not yet old enough to do so, we've designed a neutral, industry-standard age gate that requires people to fill in their complete birthdate to discourage people from simply clicking a pre-populated minimum age. For accounts banned or restricted because we believe the account holder is under a particular minimum age, the account holder can appeal. See here and here for more information. TikTok continues to investigate industry standards and best practices when considering other options for users to submit age information.

ALGORITHMIC RECOMMENDER SYSTEMS, HELP FEATURES AND ACCESS TO MENTAL HEALTH-RELATED CONTENT

As a platform used by millions of people in the US and more than 1 billion people around the world, we're committed to protecting our community every day. TikTok removes content that violates our Community Guidelines and offers features that help people explore TikTok safely, including:

- Redirecting searches linked to terms like #eatingdisorders or #suicide to prompt people to view support resources, such as helplines along with information on how they can seek assistance.
- Enabling people to refresh their feed if they feel what they are seeing is no longer relevant to them
- Using keywords to tailor their feeds to avoid potentially triggering content

TikTok cares deeply about the well-being of our community members and wants to be a source of happiness, enrichment, and belonging. We welcome people coming together to find connections, participate in shared experiences, and feel part of a broader community. We work to make sure this occurs in a supportive space that does not negatively impact people's physical or psychological health. To accomplish this, we work with our internal experts, and external partners, such as Digital Wellness Lab, Crisis Text Line, Butterfly Foundation, and the International Association for Suicide Prevention, to shape our approach to mental health content. Research shows that content related to mental health impacts different people in different ways. Nonetheless, TikTok puts limits on certain types of mental health content that can appear on the platform

We want TikTok to be a place where people can discuss emotionally complex topics in a supportive way without increasing the risk of harm and we also want to ensure that TikTok encourages self-esteem and does not promote negative social comparisons. Our Community Guidelines have a range of policies that are designed to ensure that emotionally complex topics can be discussed in a supportive way without increasing the risk of harm. For example, we do not allow showing, promoting or sharing plans for suicide, nor do we allow showing or promoting of disordered eating or any dangerous weight loss behaviors. We also take steps to age restrict content related to certain topics, like cosmetic surgery, that may promote negative social comparison in younger users. We also interrupt repetitive patterns, so that content that may be fine if seen occasionally, like extreme fitness or dieting content, is not being viewed in clusters that may be more problematic.

TikTok uses a combination of machine and human moderation to identify suitable candidates for effective signposting of resources and evaluates these search terms in accordance with TikTok's policy frameworks. We also actively solicit feedback from external organizations, such as the International Association for Suicide Prevention, Samaritans, Comentzar de Nuevo, and others to identify emerging terms that could benefit from resource signposting.

As part of TikTok's commitment to safety, education, and uplifting our community and partners, we launched a Mental Health Media Education Fund and donated over $2 million in ad credits to organizations working on supporting mental well-being, including:

- **Alliance for Eating Disorders (**@allianceforeD**)** - National Alliance for Eating Disorders is a nonprofit organization providing education, referrals, and support
- **American Foundation for Suicide Prevention (**@afspnational**)** - American Foundation for Suicide Prevention, Saving lives + bringing hope

- **Crisis Text Line (**@crisistextline**)** - Crisis Text Line provides free, 24/7 mental health support. Text TIKTOK to 741741
- **Made of Millions (**@madeofmillions**)** - Made of Millions is a global advocacy nonprofit on a mission to change how the world perceives mental health
- **National Alliance on Mental Illness (**@nami**)** - National Alliance on Mental Illness helps Americans affected by mental illness
- **National Eating Disorders Association (**@neda**)** - NEDA supports those affected by eating disorders, and serves as a catalyst for prevention, cures and access to quality care
- **Peer Health Exchange (**@peerhealthexchange**)** - Peer Health Exchange provides youth with support, resources, and education to make healthy decisions

As part of this initiative, we're also hosting a series of TikTok training sessions to equip our partners with the tools they need to share information with their communities during critical moments, such as World Mental Health Day in October or back-to-school season. This collaboration represents just one part of our continued efforts to advocate for positive mental health and reach people in need of support, and we're grateful that nonprofits and advocacy groups choose TikTok as a platform to share their knowledge and to reach a wide audience.

Encouraging Supportive Conversations
To accompany our Media Education Fund, we also launched a #MentalHealthAwareness hub for our community to easily learn about well-being topics, connect with advocates, and support organizations that provide important resources.

#MentalHealthAwareness Creator Spotlight
TikTok is a vibrant and welcoming place, enabling creators and the wider community to share their personal stories. Whether they're advocating for more open discussion about depression and anxiety or sharing tips on how people can manage body or self-esteem issues, creators in the #MentalHealthAwareness community help foster open, honest, and authentic conversations. During Mental Health Awareness Month, we spotlighted 10 creators who use TikTok to educate the community on #MentalHeathAwareness and have made a significant impact both on and off the platform over the past year.

In closing, we want to reiterate TikTok's commitment to protecting all members of our community, especially our younger users. Our continued dialogue with Amnesty International is critical as TikTok works to build trust and improve our overall approach to providing young people with an experience that is developmentally appropriate and helps to ensure a safe space for self-exploration

We thank you for your questions and appreciate the opportunity to provide additional details as needed.

With warm regards,
TikTok Trust & Safety

ANNEX 3. TIKTOK'S WRITTEN RESPONSE OF 29 OCTOBER 2023

TikTok response page 1

October 29, 2023

Lauren Dean Armistead, Head of the Children's Digital Rights Team (Interim)
Rasha Abdul Rahim, Director of Amnesty Tech
Michael Kleinman, Director of Silicon Valley Initiative
Amnesty International
1 Easton Street
London, WC1X, ODW
United Kingdom

Dear Ms. Armistead, Ms. Abdul Rahim and Mr. Kleinman,

Thank you for letter dated October 12, 2023, in which you invite TikTok to respond to Amnesty International's research reports regarding TikTok's corporate responsibility to respect human rights in relation to children and young people's use of the TikTok platform. We appreciate the opportunity to address this important topic and reaffirm our deep commitment to protecting the human rights, safety and well-being of people under the age of 18 on the platform. To that end, we would like to share more about TikTok's efforts across the themes highlighted in your report findings:

Privacy and Advertising Policies

At TikTok, the privacy and security of our users is among our highest priorities. We take our responsibility to safeguard people's privacy and data security seriously. In line with industry practices, we collect information that users choose to provide to us and share with the broader TikTok community, as well as information that helps the app function, operate securely, and improve the user experience. We detail the information we collect in our privacy policies. There are a number of inaccuracies about our practices described in the reports that we would like to clarify.

Report 1's assertions centered on TikTok's data collection practices do not accurately describe TikTok's privacy practices, nor the platform's capabilities. The TikTok app has its own built-in search engine functionality and does not directly collect what people search for outside of the app or through other search engines. TikTok does not collect precise geolocation in the US, European Economic Area, UK and many other regions. In regions where we do collect precise geolocation, we obtain consent prior to collection and people can revoke this consent at any time.

In addition to the inaccuracies described above, the assertions about LGBTQ+ content made by the *The Wall Street Journal* and referenced in the report are incorrect, as we said at the time. TikTok does not identify individuals or infer sensitive information such as sexual orientation or race based on what they watch. Additionally, as we explained to the *The Wall Street Journal*, watching a video is not necessarily a sign of someone's

identity. There are many reasons someone may engage with content; there are allies who engage with LGBTQ+ content but may not identify as LGBTQ+ themselves. There are people who enjoy baking content but aren't bakers. There are people who watch sports content and aren't athletes. People come to TikTok to discover new, entertaining content.

When we build products and features for our platform, we do so by keeping privacy in mind and building in privacy principles throughout the product development lifecycle. We also believe it's important to ensure strong protections to help keep minors and young people safe, which is why we've introduced privacy features and tools to support age-appropriate experiences on our platform. In our previous letter and above, we provided an overview of the global default protections, tools and guidance we have implemented to protect teen privacy and keep them safer on the platform. We will continue this important work.

Report 1 also inaccurately describes our ads practices. First, TikTok prohibits advertisers from using our ads products to discriminate against people unlawfully. We provided our Anti-Discrimination Ads Policy in our prior letter, which describes our stance on discriminatory ads. The report inaccurately characterizes our enforcement of this policy. All advertisements on TikTok are subject to our Community Guidelines and Advertising Policies. As a result, advertisements are not permitted if they violate TikTok's policies. Second, we implemented restrictions regarding the types of data that can be used to show ads to teens by region in an announcement in July of 2023. This policy has been implemented and we will continue to move toward providing our community with transparency and controls so they can choose the experience that's right for them.

Human Rights

TikTok is committed to respecting the human rights of all people, especially community members between the ages of 13-17. Our commitment to human rights, available on our website, is informed by several international human rights frameworks which we have pledged to uphold. These include the International Bill of Human Rights (which includes the Universal Declaration of Human Rights [UDHR], the International Covenant on Civil and Political Rights [ICCPR], and the International Covenant on Economic, Social and Cultural Rights [ICESCR]), (2) the International Labour Organization [ILO] Declaration on Fundamental Principles and Rights at Work, (3) the Convention on the Rights of the Child [CRC], and (4) the United Nations Guiding Principles on Business and Human Rights [UNGPs].

TikTok consults with a range of stakeholders to inform our human rights due diligence. For instance, we are implementing a number of recommendations to our trust and safety operations that have resulted from our engagement with Article One Advisors on human rights. These recommendations are implemented by our platform fairness team in partnership with a human rights working group of colleagues on teams across the company. The assessment recommended that TikTok to conduct a child rights impact

assessment, which we will be launching in partnership with Article One. Another recommendations was to develop a company-wide human rights due diligence process which will include conducting periodic human rights impact assessments. In partnership with Business for Social Responsibility (BSR), we are developing this human rights due diligence toolkit which will propose the triggers around when we need to conduct an assessment. This toolkit and corresponding processes are aligned with international human rights standards, most notably the UNGPs.

Finally, as your report correctly indicates, we have embedded a human rights approach across our Community Guidelines and have advisory councils around the globe, which include experts in children's rights. We are members of the WeProtect Global Alliance and the Tech Coalition. TikTok recently announced the formation of our Youth Council, which will enable us to listen to the experiences of those who directly use our platform and be better positioned to make changes to create the safest possible experience for our community. We've been working to build the council with youth representing a diversity of backgrounds and geographies and will keep Amnesty Tech informed as work progresses.

Teen Safety and Mental Health

TikTok is committed to ensuring the safety and well-being of our teenage community members. We strive to navigate the complexity of supporting our community's well-being on our platform with nuance. We take a four-pronged approach that involves removing harmful content, age-restricting or dispersing content that may not suitable for younger members of the community, and empowering people by providing them with tools and connecting them to resources. Our Community Guidelines do not allow content that shows, promotes, or shares plans for suicide or self-harm or content that shows or promotes disordered eating or any dangerous weight loss behavior. We also age-restrict certain topics that may pose unique risks to children, such as videos showing or promoting cosmetic surgery that do not include risk warnings, including before-and-after images, videos of surgical procedures, and messages discussing elective cosmetic surgery.

As the report references, TikTok has developed and implemented systems that limit content related to certain topics that may be fine if seen occasionally, but potentially problematic when presented in aggregate. These systems include coverage for topics like misery, hopelessness, sadness, and diet and fitness. We continue to work on expanding and implementing these systems, including adding more mental health topics.

We regularly consult with health experts, remove content that violates our policies, and provide access to supportive resources for anyone in need, including children. We are mindful that triggering content is unique to each individual and remain focused on fostering a safe and comfortable space for everyone, including people who choose to share their recovery journeys or educate others on these important topics. We have

published a guide for creators with suggestions on how to talk about mental health while keeping themselves safe and being respectful to other community members.

TikTok also offers tools to help parents and younger members of our community manage their screen time. As referenced in your report findings, TikTok automatically sets a 60-minute screen time limit for every account belonging to a user below age 18. Before adopting this feature and choosing this limit, we consulted academic research and experts from the Digital Wellness Lab at Boston Children's Hospital. As your report mentions, teens are able to continue watching after the 60-minute limit is reached by entering a passcode. We have found that enacting more restrictive screen time controls may increase the risk of teens lying about their age, while the passcode feature requires teens to make an active decision to extend their screen time. The interruption introduces friction into the experience, which gives people an opportunity to pause and reflect on whether they wish to continue watching. Additionally, our Family Pairing features allow parents to customize the daily screen time limit for their teens and implement stricter standards if they feel it is needed. We are monitoring the efficacy of the time limit default and are continuing to innovate to make it more effective.

In addition to Family Pairing, TikTok offers a wealth of resources for parents and guardians to help safeguard their teen's safety, privacy, and well-being on the platform, which can be found directly in TikTok's Safety Center. Additionally, TikTok's Youth Portal offers both in-app tools and educational content that empower young users to keep their account secure and limit their online footprint to the degree they feel comfortable. The Youth Portal includes a "You're in Control" video series which provides safety and security tips for all users.

TikTok is committed to upholding human rights and maintaining a safe platform for all members of our community, especially our younger users. We appreciate the opportunity to respond to these reports and welcome a continued dialogue on these important issues.

Sincerely,

Lisa Hayes
Head of Safety Public Policy & Senior Counsel, Americas, TikTok

AMNESTY INTERNATIONAL IS A GLOBAL MOVEMENT FOR HUMAN RIGHTS. WHEN INJUSTICE HAPPENS TO ONE PERSON, IT MATTERS TO US ALL.

CONTACT US

info@amnesty.org

+44 (0)20 7413 5500

JOIN THE CONVERSATION

www.facebook.com/AmnestyGlobal

@amnesty

“I FEEL EXPOSED”

CAUGHT IN TIKTOK’S SURVEILLANCE WEB

TikTok’s highly personalized ‘For You’ feed has helped it to become, in the space of a few years, one of the most popular social media platforms in the world with over 1 billion users, many of whom are children between the ages of 13 and 17. But behind the never-ending feed of lip-syncing and dance craze videos is a highly extractive business model based on the collection of massive amounts of personal data on each user’s behaviour on the platform and in some parts of the world, their activity off the platform, as well as in the physical world.

TikTok has introduced some changes to ensure greater respect of children’s rights, but they differ from region to region. This differential treatment for child users in some parts of the world is discriminatory and TikTok should immediately extend the same rights-respecting policies to all child users globally.

The failure of TikTok to put in place adequate policies to respect the rights of children shows that stronger laws and regulation on data protection and algorithmic amplification of content on social media, as well as effective enforcement, is needed to keep children safe. It is essential that states move quickly to introduce and enforce comprehensive laws to rein in their surveillance-based business models.

INDEX: POL 40/7349/2023
OCTOBER 2023
LANGUAGE: ENGLISH

amnesty.org

AMNESTY INTERNATIONAL