



BREAKING UP WITH BIG TECH

A HUMAN RIGHTS-BASED ARGUMENT FOR TACKLING BIG TECH'S
MARKET POWER

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.

© Amnesty International 2025

Except where otherwise noted, content in this document is licensed under a Creative Commons (attribution, non-commercial, no derivatives, international 4.0) licence.

<https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>

For more information please visit the permissions page on our website: www.amnesty.org

Where material is attributed to a copyright owner other than Amnesty International this material is not subject to the Creative Commons licence.

First published in 2025

by Amnesty International Ltd

Peter Benenson House, 1 Easton Street
London WC1X 0DW, UK

Index: POL 30/0226/2025

Original language: English

amnesty.org



Cover illustration: Graphic Design by Charlie Messenger

AMNESTY
INTERNATIONAL



CONTENTS

1. EXECUTIVE SUMMARY	4
2. BIG TECH MARKET POWER	6
2.1 GOOGLE AND META	6
2.2 MICROSOFT	9
2.3 AMAZON	10
2.4 APPLE	11
3. HUMAN RIGHTS HARMS OF BIG TECH'S MARKET POWER	13
3.1 EXCESSIVE DATA COLLECTION AND THE RIGHT TO PRIVACY	13
3.2 IMPOSITION OF UNFAIR TERMS AND CONDITIONS	15
3.3 AMPLIFICATION OF HARMFUL CONTENT	18
3.4 FREEDOM OF EXPRESSION, OPINION AND ACCESS TO INFORMATION	20
3.5 CROWDING OUT THE POTENTIAL FOR RIGHTS-RESPECTING ALTERNATIVES	23
3.6 LABOUR RIGHTS ABUSES	24
3.7 REGULATORY CAPTURE AND INFLUENCE	27
4. THE NEXT PHASE: DOMINANCE IN GENERATIVE ARTIFICIAL INTELLIGENCE	30
5. THE ROLE OF COMPETITION LAW IN STATES' HUMAN RIGHTS OBLIGATIONS	33
6. CONCLUSION AND RECOMMENDATIONS	35
ANNEX	37

1. EXECUTIVE SUMMARY

In today's digital age, a small group of technology giants – Alphabet (Google), Meta, Microsoft, Amazon, and Apple – wield extraordinary influence over the infrastructure, services, and norms that shape our online lives. These companies dominate key sectors of the internet: from search and social media to cloud computing, e-commerce, and mobile operating systems. While not all their market positions constitute illegal monopolies, their collective market power enables them to set the terms of digital engagement for billions of people worldwide. Their reach is so extensive that some experts have even likened them to utility providers.¹ This concentration of power has profound implications for human rights, particularly the rights to privacy, non-discrimination, and access to information.

Google and Meta's market dominance is built on pervasive surveillance. By harvesting and monetizing vast quantities of our personal data, they have entrenched a business model that thrives on profiling, behavioural prediction, and algorithmic targeting. This model not only undermines the right to privacy but also reinforces their market power in a self-perpetuating cycle: the more data they collect, the more dominant they become, and the harder it is for competitors to challenge their position. The result is a digital ecosystem where users have little meaningful choice or control over how their data is used.

Beyond privacy concerns, Big Tech's dominance can also lead to devastating consequences for marginalized communities. Platforms like Facebook, Instagram and YouTube have become primary gateways to news and public discourse. Their algorithmic systems – optimized for engagement and profit – have been shown to amplify harmful content which elicits a stronger reaction from users and keeps us online longer, allowing these companies to collect more data on us and serve us more adverts. In an increasingly polarized context, this can contribute to the rapid spread of discriminatory speech and even incitement to violence – which has had devastating consequences in several crisis and conflict-affected areas.

The dominance of Big Tech also poses serious risks to freedom of opinion and access to information. Social media platforms shape what millions of people see online, often through opaque algorithms that prioritize engagement over accuracy or diversity. In many countries, these platforms have become so embedded in daily life that meaningful participation in society often depends on using their services. This gives them enormous power to influence public discourse and curate information flows. Documented cases of content removal, inconsistent moderation, and algorithmic bias highlight the dangers of allowing a handful of companies to act as gatekeepers of the digital public sphere.

Moreover, the dominance of these firms has enabled them to impose unfair terms and conditions on users, crowd out the market potential for rights-respecting alternatives, and exert disproportionate influence over regulatory processes. Their lobbying power, strategic acquisitions, and control over essential digital infrastructure and markets has created barriers to accountability and legislative reform. As these companies expand their product offerings to include generative AI, their existing advantages in terms of data access and political influence threaten to further entrench their dominance in the next frontier of technological development.

¹ Josh Simons and Dipayan Ghosh, *Utilities for Democracy: Why and How the Algorithmic Infrastructure of Facebook and Google Must Be Regulated*, August 2020, <https://www.brookings.edu/articles/utilities-for-democracy-why-and-how-the-algorithmic-infrastructure-of-facebook-and-google-must-be-regulated>

This briefing demonstrates that addressing Big Tech’s dominance is not only a matter of market fairness but a pressing human rights issue. It outlines:

- How the “Big Five” tech companies have accumulated and maintained market power.
- The human rights harms linked to their dominance, including violations of privacy, access to information, freedom of opinion, workers’ rights, and freedom from non-discrimination.
- How Big Tech companies are threatening to further embed systems that harm our rights through their expansion into the generative Artificial Intelligence (AI) market.
- The role of competition law as a powerful but underutilized tool for states to meet their human rights obligations under international law.

Competition law, applied with a human rights lens, can serve to dismantle harmful concentrations of power and act as a powerful tool for states to implement their human rights obligations under international law. The briefing concludes with a set of recommendations for states and competition regulators, including the need to break up dominant firms where necessary, mandate interoperability and data portability, and ensure that competition enforcement is informed by human rights considerations. It calls for a coordinated regulatory response – one that brings together competition, data protection, consumer protection, and human rights authorities – to dismantle harmful concentrations of power and build a more pluralistic, rights-respecting digital ecosystem.

Amnesty International wrote to Meta, Google, Amazon, Microsoft and Apple on 12 August 2025 with a summary of the relevant findings contained in this briefing. Meta and Microsoft responded in writing. Their responses are referenced throughout this report where relevant and included in full in the annex. Google, Amazon, and Apple had not responded ahead of the publication deadline.

2. BIG TECH MARKET POWER

Outside of China, which has its own largely separate ecosystem of digital services providers, the online world is dominated in large part by five companies, collectively known as “Big Tech” – Google, Meta, Microsoft, Amazon and Apple. Recently designated as “gatekeepers” of digital markets by the EU, each of these companies holds significant market share in different digital markets: Google in search, video, web browsing, mobile (operating systems and app distribution), and online advertising; Meta in social media, messaging services and online advertising; Microsoft in cloud, productivity software and desktop operating systems; Amazon in e-commerce and cloud; and Apple in mobile (smartphones, operating systems and app distribution) and health and fitness tracking.²

This section outlines how the significant market power of these Big Tech companies was built. Not all of these dominant positions are considered illegal monopolies; however, these companies do hold significant collective power over our use of and access to the internet, the conditions under which users can engage with the internet, and internet services which can have profound human rights implications.

2.1 GOOGLE AND META

As outlined in Amnesty International’s report *Surveillance Giants*, Google and Meta have come to gain unparalleled power over people’s lives online.³ These two companies, and the various companies they own, including Facebook, YouTube and WhatsApp, mediate the ways people seek and share information, engage in debate, and participate in society.⁴ They have established control over the main channels that most of the world relies on to engage with the internet and have become fundamental to the modern world and how people interact with one another.⁵

Facebook has 3.07 billion monthly active users; that’s roughly three in every eight people on the planet and Facebook is just one of Meta’s services.⁶ WhatsApp and Instagram have 2 billion users apiece, meaning Meta owns three of the top four social media platforms by user numbers.⁷ Google’s YouTube is not far behind with around 2.5 billion users – the second highest number of monthly active users of any social media platform – and there are an estimated 13.7 billion searches on Google Search every day.⁸

Google and Meta’s market power is intrinsically linked to data.⁹ Their business models are predicated first and foremost on the extraction and accumulation of vast amounts of data so that they can serve users highly

² European Commission, “Gatekeepers”, 6 September 2023, https://digital-markets-act.ec.europa.eu/gatekeepers_en (accessed on 1 August 2025).

³ 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/wp-content/uploads/2021/05/POL3014042019ENGLISH.pdf>

⁴ Please note that we use Google throughout to refer to Google’s parent company Alphabet Inc.

⁵ Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights* (previously cited).

⁶ Jake Lerch, “How Meta platforms dominates the internet, explained in 1 chart”, 6 March 2024, <https://www.fool.com/investing/2024/03/06/how-meta-platforms-dominates-the-internet-explaine>

⁷ Jake Lerch, “How Meta platforms dominates the internet, explained in 1 chart” (previously cited).

⁸ DemandSage, “How Many Google Searches Per Day [2025 Data]”, 22 May 2025, <https://www.demandsage.com/google-search-statistics/>

⁹ Facebook stated in 2019 that its business is not driven by the collection of data about people, and data collection is not an end in itself for the company, but that Facebook is supported through the sale of advertising. See Amnesty International, “*Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights*” (previously cited) for Facebook’s full response, pp. 51-56.

personalized content and advertising, through a practice called profiling.¹⁰ Meta and Google are not only collecting our data, but they can also use that data to infer and create new information about us.¹¹ The platforms are underpinned by state-of-the-art artificial intelligence and machine learning tools that infer detailed characteristics about users and group them into highly specific categories for targeted advertising.¹²

Google and Meta are not charging us for all their services,¹³ because they are earning money off our data. Google's advertising infrastructure is embedded in millions of websites,¹⁴ and its Android operating system grants Google access to data from millions of smartphones worldwide.¹⁵ This allows Google to collect not only search queries and browsing history, but also granular behavioural data – such as how long users linger on a page, their physical location and even their social interactions.¹⁶ Meta similarly monitors user activity both on and off its platforms, including users who don't necessarily have an account with them, through agreements with third parties.¹⁷

To increase their revenue from advertisers, these companies compete to offer the best predictions about the most people. To achieve this, they continually expand their data collection and refine their predictive algorithms. This incentivises the companies to seek more and more data on more people and to expand their operations across the internet, across the world, and in physical space through smart appliances and devices.¹⁸

Meta and Google's expansive data collection is in part conducted through providing services to other companies. For instance, when third-party companies use Google services such as Google Sign-in, Google Analytics, AdSense, or embed video content from YouTube on their websites, these sites and apps agree to share user information with Google.¹⁹ Similarly, Meta's agreements with third parties through cookies and services vastly increase its access to information about our use of the internet. In exchange for services such as "login with Facebook", which allows users to access third-party websites or apps using their Facebook login details;²⁰ "Meta Pixel", which provides companies with website analytics;²¹ and social plugins including share and like buttons,²² Meta's clients provide it with access to data on who visits their websites.²³

Google and Meta's market power is further reinforced through strategic acquisitions – particularly those that provide access to valuable user data. Meta's purchases of Instagram and WhatsApp, for example, not only eliminated emerging rivals but also expanded their surveillance reach across different modes of communication and social interaction.²⁴ Google's acquisitions of YouTube, Fitbit, and advertising technologies such as DoubleClick have enabled the company to consolidate vast datasets across video, health, and ad ecosystems. For example, the Google and Fitbit merger in 2021 gave Google access to health

¹⁰ Google generated 75% of total revenue from advertising in 2024; Alphabet Inc., *2024 Annual Report*, 31 January 2025, <https://abc.xyz/assets/70/a3/43ba8a804b49ac2fa2595c3c6704/2024-annual-report.pdf>; Meta generated 97.6% of total revenue from advertising in 2024 Meta Platforms, Inc., "Form 10-K (fiscal year ended December 31, 2024)", 1 February 2024, <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/a8eb8302-b52c-4db5-964f-a2d796c05f4b.pdf>

¹¹ Privacy International, "Examples of Data Points Used in Profiling", April 2018, https://privacyinternational.org/sites/default/files/2018-04/data%20points%20used%20in%20tracking_0.pdf;

Facebook stated in 2019 that it does not infer people's sexual identity, personality traits, or sexual orientation. See Amnesty International, "Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights" (previously cited) for Facebook's full response, pp. 51-56.

¹² Andrew Hutchinson, "Meta outlines its evolving AI ad targeting process, which is improving ad performance", 12 May 2023, <https://www.socialmediatoday.com/news/meta-outlines-evolving-ai-ad-targeting-process-improving-ad/650225/>; ODSC Team, "Meta plans full AI automation of ads by 2026 amid competitive ad tech push", 2 June 2025, <https://opendatascience.com/meta-plans-full-ai-automation-of-ads-by-2026-amid-competitive-ad-tech-push>; Privacy International, "Examples of Data Points Used in Profiling" (previously cited)

¹³ Some Google and Meta services are funded through other means such as subscriptions but both companies provide services that are primarily free to the end user and funded by advertising.

¹⁴ BuiltWith, "DoubleClick.Net Usage Statistics", <https://trends.builtwith.com/ads/DoubleClick.Net> (accessed 1 August 2025).

¹⁵ Google, Privacy Policy, 1 July 2025, <https://policies.google.com/privacy?hl=en> (accessed 1 August 2025).

¹⁶ Google, Privacy Policy (previously cited).

¹⁷ Google, Privacy Policy (previously cited).

¹⁸ Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights* (previously cited).

¹⁹ Google, How Google uses information from sites or apps that use our services, 1 July 2025, <https://policies.google.com/technologies/partner-sites?hl=en-US> (accessed 1 August 2025).

²⁰ Meta for Developers, Facebook Login, 20 August 2025, [Facebook Login | Facebook for Developers](https://developers.facebook.com/docs/facebook-login/) (accessed 20 August 2025).

²¹ Meta for Developers, Meta Pixel, <https://developers.facebook.com/docs/meta-pixel/> (accessed 1 August 2025).

²² In Facebook's response to *Surveillance giants*, it clarified that "other than for security purposes and guarding against fraud, Facebook no longer stores data from social plugins (such as the Like Button) with user or device identifiers." However, Meta's Privacy Policy states: "We collect and receive information from partners, measurement vendors, marketing vendors and other third parties about a variety of your information and activities on and off our products... (including) Websites that you visit and cookie data, such as through Social plugins or the Meta pixel"; Meta, Information from partners, vendors and other third parties, <https://www.facebook.com/privacy/policy?subpage=1.subpage.4-InformationFromPartnersVendors> (accessed 30 July 2025).

²³ Meta, Information from partners, vendors and other third parties (previously cited).

²⁴ Federal Trade Commission, "FTC alleges Facebook resorted to illegal buy-or-bury scheme to crush competition after string of failed attempts to innovate", 19 August 2021, <https://www.ftc.gov/news-events/news/press-releases/2021/08/ftc-alleges-facebook-resorted-illegal-buy-or-bury-scheme-crush-competition-after-string-failed>

data that had previously been inaccessible.²⁵ Meta's purchase of mobile analytics company Onavo Inc. in 2013²⁶ provided it with access to data analytics on the performance of apps including Meta's competitors at a time when Meta was attempting to break into the smartphone market.²⁷ Meta was even alleged to have used this newly acquired technology through the Onavo purchase to "wiretap" encrypted data to monitor competitor traffic analytics.²⁸

Meta and Google's dominance in their respective digital markets is also *reinforced* by their extensive data collection. In the digital economy, the value of personal data increases as more is collected and combined. This is because the ability of companies to target advertising effectively increases with more data, or at the very least, advertisers perceive this to be so. This creates a powerful incentive for companies to pursue business strategies aimed at collecting as much data as possible.²⁹ Google and Meta's acquisitions have allowed them to integrate and cross-reference user data from multiple sources, deepening their individual profiling capabilities and reinforcing their market power.

Meta's dominance is also reinforced by network effects: the more people that use a platform, the more valuable it becomes to others. Users are more likely to remain active on platforms that their friends, family, and communities use.³⁰ This dynamic also makes it difficult for alternative platforms to gain traction.

The US Federal Trade Commission (FTC) – an independent agency responsible for protecting consumers and promoting competition – has accused both Google and Meta of engaging in anti-competitive practices to increase their dominance in various digital markets.³¹ Google's purchase of various digital advertising companies, for example, means it now controls every stage of the online advertising process. Google has been accused of eliminating competitors through a series of acquisitions and anti-competitive practices, such as unlawfully tying its publisher advertising platform (DoubleClick for Publishers) to its advertising exchange (AdX).³² In relation to Google's search function, the US Department of Justice (DOJ) has also accused Google of "(entering) into a series of exclusionary agreements that collectively lock up the primary avenues through which users access search engines, and thus the internet."³³ The FTC has now ruled both Google's advertising technology and its general internet search function to be illegal monopolies.³⁴ At the time of writing, the decisions on proposed remedies in these cases had not been made.

In 2020, the FTC filed a claim against Meta that accused the company of accumulating monopoly power in social networking through anti-competitive practices, including "buy or bury" tactics.³⁵ The FTC alleged that Meta bought competitors Instagram (2012) and WhatsApp (2014) when these companies became a threat to Meta's dominance in social media networking, and that Meta imposed anti-competitive conditions on third-party developers, restricting their ability to compete or interoperate with the Facebook platform.³⁶ The alleged conduct includes requiring competitors, through contracts, to agree not to build features that compete with Facebook's core functions or connect with other social media platforms.³⁷ At the time of

²⁵ Michael Allison, "After a few hurdles, Google's \$2.1 billion Fitbit acquisition is finally complete", 14 January 2021, Android Central, <https://www.androidcentral.com/googles-fitbit-acquisition-finally-complete>;

At the time Google stated that the merger was not about data, but a year after the merger Google announced that it would begin merging Fitbit accounts with Google accounts.

²⁶ Ingrid Lunden, "Facebook buys mobile analytics company Onavo and finally gets its office in Israel", 13 October 2013, Tech Crunch, <https://techcrunch.com/2013/10/13/facebook-buys-mobile-analytics-company-onavo-and-finally-gets-its-office-in-israel/>

²⁷ Internal documents revealed that Meta (then Facebook) used Onavo to collect encrypted data on competitors including Snapchat, Amazon and YouTube; Lorenzo Franceschi-Bicchieri, "Facebook snooped on users' Snapchat traffic in secret project, documents reveal", 26 March 2024, Tech Crunch, <https://techcrunch.com/2024/03/26/facebook-secret-project-snooped-snapchat-user-traffic/>

²⁸ US District Court for the Northern District of California, *Klein v Meta Platforms, Inc.*, Facebook/Meta class action discovery, 31 May 2023, <https://www.documentcloud.org/documents/24520332-merged-fb>

²⁹ World Economic Forum, *Personal Data: The Emergence of a New Asset Class*, 17 February 2011, https://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

³⁰ Investopedia, "What Is the Network Effect?", 22 August 2024, <https://www.investopedia.com/terms/n/network-effect.asp>

³¹ US District Court for the District of Columbia, *State of New York, et al. v Facebook, Inc.*, Executive Summary of Plaintiffs' Revised Proposed Final judgment, 3 July 2025, <https://www.justice.gov/atr/case/state-new-york-et-al-v-facebook-inc>; US Department of Justice, "Department of Justice prevails in landmark antitrust case against Google", 17 April 2025, <https://www.justice.gov/opa/pr/departments-justice-prevails-landmark-antitrust-case-against-google>

³² US Department of Justice, "Justice Department sues Google for monopolizing digital advertising technologies", 24 January 2023, <https://www.justice.gov/archives/opa/pr/justice-department-sues-google-monopolizing-digital-advertising-technologies>

³³ US Department of Justice, "Justice Department sues monopolist Google for violating antitrust laws", 20 October 2020, <https://www.justice.gov/archives/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws>

³⁴ US District Court for the District of Columbia, *State of New York, et al. v Facebook, Inc.*, Executive Summary of Plaintiffs' Revised Proposed Final judgment" (previously cited); US Department of Justice, "Department of Justice prevails in landmark antitrust case against Google" (previously cited).

³⁵ Federal Trade Commission, "FTC alleges Facebook resorted to illegal buy-or-bury scheme to crush competition after string of failed attempts to innovate" (previously cited).

³⁶ Federal Trade Commission, "FTC alleges Facebook resorted to illegal buy-or-bury scheme to crush competition after string of failed attempts to innovate" (previously cited).

³⁷ On July 27 2011, Facebook introduced a policy regarding actions that apps accessing the Facebook Platform could take: "Apps on Facebook may not integrate, link to, promote, distribute, or redirect to any app on any other competing social platform." United States District Court for the District of Columbia, Executive summary of plaintiffs' revised proposed final judgment (previously cited).

writing, there is a decision pending as to whether these actions were an “abuse of dominance” and considered anti-competitive practices. Should these findings be made, Meta could be required by the FTC to divest from Instagram and WhatsApp and be prohibited from imposing anti-competitive conditions on software developers.

2.2 MICROSOFT

Microsoft’s dominance was first challenged in the early 2000s during the so-called “browser wars,” when it bundled Internet Explorer with its Windows operating system. This practice was found to be anti-competitive, as it effectively shut out rival browsers.³⁸ One competitor, Netscape (now Mozilla Foundation), responded by open sourcing their browser Firefox and giving it away for free, which broke Microsoft’s dominance in the browser market and led to greater consumer choice.³⁹ Microsoft’s current browser – Microsoft Edge – now has less than 12 percent share of global browser usage.⁴⁰

Despite this outcome on browsers, Microsoft’s dominant position in desktop operating systems and productivity software (e.g. Windows and Office) has remained largely unchallenged. Windows remains the leading desktop operating system worldwide, with a global market share of approximately 72% as of early 2025, and these products continue to be deeply embedded in public and private sector infrastructure globally.⁴¹ Microsoft also holds public sector contracts across the world.⁴² For example, in 2024, Microsoft held over 280 contracts with the US government, including as a key cloud and software provider for US government defence and intelligence agencies.⁴³

In recent years, Microsoft has also integrated artificial intelligence (AI), cloud computing, and communication tools (such as Microsoft Teams) into its tightly coupled ecosystem.⁴⁴ Amnesty International wrote to Microsoft on 12 August 2025 to enquire about this practice and Microsoft replied that “Windows and Azure are both open platforms that enable customers to use them as interoperable tools”.⁴⁵ However, this bundling of services creates high switching costs for users, reinforcing dependency on Microsoft’s suite of products. The result is an environment that is difficult for competitors to penetrate; a situation that has been investigated by the EU as a potentially anti-competitive practice.⁴⁶

Microsoft Azure, the company’s cloud computing infrastructure, is currently the second-largest cloud platform globally, behind only Amazon Web Services (AWS). Microsoft’s market share in cloud continues to grow rapidly and could overtake Amazon in 2026 if current trends continue.⁴⁷ Microsoft’s early investment in generative AI, most notably through its \$10 billion partnership with OpenAI starting in 2019,⁴⁸ has positioned the company to potentially dominate this next wave of technological development. By embedding AI capabilities into its cloud and productivity tools, Microsoft is not only expanding its reach but also shaping the infrastructure on which future digital services will depend.

³⁸ US Court of Appeals for the District of Columbia Circuit, *U.S. v. Microsoft Corp.*, 253 F.3d 34 (D.C. Cir. 2001) 28 June 2001, <https://law.justia.com/cases/federal/appellate-courts/F3/253/34/576095>

³⁹ Netscape Communications (archived), “Netscape announces plans to make next-generation communicator source code available free on the net”, 22 January 1998, <https://web.archive.org/web/20021001071727/wp.netscape.com/newsref/pr/newsrelease558.html>

⁴⁰ Statcounter, Desktop Browser Market Share Worldwide (July 2024 - July 2025) <https://gs.statcounter.com/browser-market-share/desktop/worldwide> (accessed 26 August 2025)

⁴¹ Coolest Gadgets, “Operating Systems Statistics by Usage, Users and Revenue (2025)”, 10 February 2025, <https://coolest-gadgets.com/operating-systems-statistics>

⁴² For example, Microsoft, “New agreement with Microsoft supports government to embrace public cloud”, 29 October 2019, <https://news.microsoft.com/en-xm/2019/10/29/new-agreement-with-microsoft-supports-government-to-embrace-public-cloud>; Microsoft, “Microsoft and G42 announce \$1 billion comprehensive digital ecosystem initiative for Kenya”, 22 May 2024, <https://news.microsoft.com/source/2024/05/22/microsoft-and-g42-announce-1-billion-comprehensive-digital-ecosystem-initiative-for-kenya>; Microsoft, Public Sector, <https://news.microsoft.com/apac/features/public-sector> (accessed 12 August 2024).

⁴³ USAspending.gov, “Federal Awards Search Results”, <https://www.usaspending.gov/search?hash=a1681132e614a82d3454ec3b7af43664> (accessed 1 August 2025).

⁴⁴ Microsoft Learn, Overview of AI in Microsoft Teams, 7 January 2025, <https://learn.microsoft.com/en-us/microsoftteams/copilot-ai-agents-overview> (accessed 1 August 2025).

⁴⁵ In their response to Amnesty International Microsoft expressed that both Microsoft Windows and Azure are open platforms that enable customers to use them as interoperable tools. Windows allows applications to be installed from any source, without the need to get Microsoft’s permission or pay a fee and Windows users can choose browsers besides Microsoft’s own browser. Azure customer can use multiple cloud services as well as available third-party apps and services. For Microsoft’s full response please refer to the annex of this briefing.

⁴⁶ European Commission, “Antitrust: Commission opens investigation into possible anticompetitive practices by Microsoft regarding Teams”, 27 July 2023, https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_23_3991/IP_23_3991_EN.pdf

⁴⁷ Forbes, “Why Microsoft Azure could take the cloud lead from Amazon AWS by 2026”, 13 February 2024, <https://www.forbes.com/sites/petercohan/2024/02/13/why-microsoft-azure-could-take-the-cloud-lead-from-amazon-aws-by-2026>

⁴⁸ Bloomberg via Yahoo Finance, “Microsoft invests \$10 Billion in ChatGPT maker OpenAI”, 23 January 2023, <https://finance.yahoo.com/news/microsoft-invests-10-billion-chatgpt-155459385.html>

2.3 AMAZON

As the world's largest e-commerce company, Amazon has become the primary gateway for online shopping in over 100 countries, serving more than 310 million active users globally.⁴⁹ Its dominant market position has enabled Amazon to exert significant control over independent sellers on the platform, who often feel they have no viable alternative but to operate within Amazon's ecosystem.⁵⁰ This power imbalance has contributed not only to rising costs for sellers, but also to documented labour rights abuses across its global operations (see section 3.6 "Labour rights abuses" for more details).

Amazon's market power stems not only from its scale, but also from its multifaceted role as a marketplace operator, service provider and direct seller. It charges sellers a range of fees – for listing items for sale, logistics (Fulfilment by Amazon), and advertising – that have steadily increased over time.⁵¹ In 2024, Amazon generated \$156.1 billion in revenue from third-party seller services alone.⁵² Advertising revenue from sellers has also surged, with Amazon reportedly prioritizing paid listings over organic search results.⁵³ These rising costs have led Amazon to capture up to 50% of sellers' revenue, squeezing their margins and forcing many to raise prices or exit the market.⁵⁴

Moreover, Amazon sellers have expressed concerns that Amazon unfairly favours its own products and sellers purchasing additional services.⁵⁵ Sellers can buy access to additional features like Buy Box – a feature that appears on product detail pages and puts products in a prominent box on the search page and allows customers to add items directly to their cart – and Prime eligibility, when a product qualifies for Amazon Prime benefits such as next day free delivery, and Pay-per-click advertising. Amazon claims that it provides non-discriminatory access to Buy Box and that participation in additional services is voluntary but Amazon sellers have expressed that purchasing these services has become "less of an option and more of a requirement for sellers to compete".⁵⁶ Investigations by the FTC and European competition authorities have also alleged that Amazon unfairly favours its own products and sellers using add-on services (such as logistics), distorting fair competition.⁵⁷

In many ways, Amazon's dominance in the e-commerce market relies on its extensive collection and analysis of data. The company collects and aggregates buyer and seller data and uses it to model behaviours, target advertising, and predict future shopping trends.⁵⁸ Sellers have also reported that Amazon uses their data to develop competing products.⁵⁹

Amazon's business model also depends on gathering data on its employees to improve efficiency and drive down costs. Workers in Amazon's "fulfilment centres" and warehouses have accused the company of subjecting them to intense surveillance. For example, in France, Amazon was fined in 2024 for excessive monitoring of employee activity. The French data protection authority (CNIL) found Amazon France Logistique tracked employee activity very precisely including systems which automatically flagged breaks of 10 minutes or more.⁶⁰ Amazon said it strongly disagreed with these findings, calling them "factually incorrect".⁶¹

⁴⁹ Yaguara, "21+ Amazon statistics 2025 (Number of users & revenue)", 12 May 2025, <https://www.yaguara.co/amazon-statistics>

⁵⁰ The Centre for Research on Multinational Corporations (SOMO), *Amazon's European Chokehold and Monopoly Power*, 14 June 2023, <https://www.somo.nl/amazons-european-chokehold> and US House of Representatives, *Investigation of Competition in Digital Markets*, October 2020, <https://www.govinfo.gov/content/pkg/CPRT-117HPRT47832/pdf/CPRT-117HPRT47832.pdf>

⁵¹ SOMO, *Amazon's European Chokehold and Monopoly Power* (previously cited); US House of Representatives, *Investigation of Competition in Digital Markets* (previously cited).

⁵² Amazon.com, Inc., "Form 10-K Annual Report for fiscal year ended December 31, 2024", 6 February 2025, <https://www.sec.gov/Archives/edgar/data/1018724/000101872425000004/amzn-20241231.htm>

⁵³ Marketplace Pulse, "Amazon is burying organic search results", 9 March 2022, <https://www.marketplacepulse.com/articles/amazon-is-burying-organic-search-results>

⁵⁴ SOMO, *Amazon's European Chokehold and Monopoly Power* (previously cited); Marketplace Pulse, "Amazon takes a 50% cut of sellers' revenue", 13 February 2023, <https://www.marketplacepulse.com/articles/amazon-takes-a-50-cut-of-sellers-revenue>

⁵⁵ US House of Representatives, *Investigation of Competition in Digital Markets*, (previously cited)

⁵⁶ US House of Representatives, *Investigation of Competition in Digital Markets*, (previously cited)

⁵⁷ Federal Trade Commission, "FTC sues Amazon for illegally maintaining monopoly power", 26 September 2023, <https://www.ftc.gov/news-events/news/press-releases/2023/09/ftc-sues-amazon-illegally-maintaining-monopoly-power>; AGCM (Italian Competition Authority), "Amazon fined over €1.128 billion for abusing its dominant position", 9 December 2021, <https://en.agcm.it/en/media/press-releases/2021/12/A528>; European Commission, "Commission opens second investigation into Amazon's e-commerce business practices", 10 November 2020, <https://ec.europa.eu/newsroom/comp/items/693430/en>

⁵⁸ US House of Representatives, *Investigation of Competition in Digital Markets*, (previously cited).

⁵⁹ European Commission, Commission Decision in case AT.40462 – Amazon Marketplace, 20 December 2022,

https://ec.europa.eu/competition/antitrust/cases1/202310/AT_40462_8990760_8322_4.pdf; US House of Representatives, *Investigation of Competition in Digital Markets*, (previously cited).

⁶⁰ BBC News, "Amazon fined for 'excessive' surveillance of workers", 23 January 2024, <https://www.bbc.co.uk/news/business-68067022>

⁶¹ BBC News, "Amazon fined for 'excessive' surveillance of workers" (previously cited).

Beyond e-commerce, Amazon has also established itself as an early leader in the market for cloud, launching its cloud infrastructure arm as early as 2006.⁶² As of July 2025, Amazon Web Services had significant market share in cloud infrastructure, holding 30% of the market – ahead of both Microsoft (21%) and Google (12%).⁶³

2.4 APPLE

Apple's market power is rooted in its wide-ranging ecosystem of hardware and software. Unlike other Big Tech firms that primarily monetize through advertising, Apple's business model is centred on the sale of devices – such as iPhones, iPads and MacBooks – combined with tightly integrated software and services.⁶⁴ Apple holds almost 60% of the smartphone operating system market in the US and just over 25% of the global market share.⁶⁵ For users already with Apple devices, exercising consumer choices becomes increasingly difficult, as Apple products are designed to work with one another, and third-party products are not usually compatible.⁶⁶ This ecosystem design creates high switching costs for users and developers alike, reinforcing Apple's position in the market. In August 2024 in the US, Apple was sued by the DOJ and a coalition of states over allegations that the company “make[s] it extremely difficult and expensive ... to venture outside the Apple ecosystem.”⁶⁷

Apple's App Store is a key pillar of its market power. As the sole gateway for app distribution on iOS devices, Apple sets the rules for developers and takes a commission of up to 30% on app sales, subscriptions and in-app purchases.⁶⁸ Apple's app store practices have drawn scrutiny from regulators. For example, in 2025, the European Commission fined Apple €1.8 billion for anti-competitive behaviour in the music streaming market, finding that Apple had restricted app developers from informing users about cheaper subscription options outside the App Store.⁶⁹

Apple's market power also extends into digital payments and health tracking. Apple Pay is now one of the most widely used mobile payment systems in the world, integrated by default into iPhones and Apple Watches.⁷⁰ In many markets, Apple restricts access to the iPhone's NFC (near-field communication) chip, preventing rival payment services from offering tap-to-pay functionality.⁷¹ This has led to an antitrust investigation in the EU and an antitrust ruling in Brazil where the Brazilian competition regulator (CADE) recommended Apple be sanctioned for the “imposition of the exclusive use of its payment system by app developers and the restriction on the distribution and commercialization of third-party digital services.”⁷²

Apple's expansion into health and fitness – through the Apple Watch and HealthKit – has also raised concerns about the company's growing access to sensitive health data.⁷³ HealthKit allows third-party apps and devices to feed data into Apple's Health app, creating a centralized repository of personal health information.⁷⁴ This includes data such as heart rate, glucose levels, sleep patterns, reproductive health, and even medical records when integrated with healthcare providers.⁷⁵ While Apple emphasizes user privacy and offers controls over what data is shared and with whom, the sheer scale and sensitivity of the data collected

⁶² Amazon, “Amazon Web Services launches”, 14 March 2006, <https://press.aboutamazon.com/2006/3/amazon-web-services-launches>

⁶³ HG Insights, “AWS market share 2025: Insights into the buyer landscape”, 19 February 2025, <https://hginsights.com/blog/aws-market-report-buyer-landscape>

⁶⁴ Financial Times, “Apple Inc. stock profile”, 18 July 2025, <https://markets.ft.com/data/equities/tearsheet/profile?s=AAPL:WSE>

⁶⁵ StatCounter, “Mobile Operating System Market Share Worldwide 2009-2023”, <https://gs.statcounter.com/os-market-share/mobile/worldwide#yearly-2009-2023> (accessed 1 August 2025); Forbes, “Apple #1 in global smartphone market for first time ever”, 16 January 2024, <https://www.forbes.com/sites/johnkoetsier/2024/01/16/apple-1-in-global-smartphone-market-for-first-time-ever>

⁶⁶ John Dudovskiy, *Apple Ecosystem: Closed and Effective*, 6 July 2023, <https://research-methodology.net/apple-ecosystem-closed-effective>

⁶⁷ CNET, “The US sues Apple over iPhone competition: What to know”, 21 March 2024, <https://www.cnet.com/tech/mobile/the-us-sues-apple-over-iphone-competition-what-to-know>

⁶⁸ AppleInsider, “Every Apple App Store fee, explained: How much, for what, and when”, 8 January 2023, <https://appleinsider.com/articles/23/01/08/the-cost-of-doing-business-apples-app-store-fees-explained>

⁶⁹ European Commission, “Commission fines Apple over €1.8 billion over abusive App Store rules for music streaming providers”, 4 March 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1161

⁷⁰ TechJury, “How Many People Use Apple Pay: 2025 Global Stats”, 2 January 2024, <https://techjury.net/industry-analysis/apple-pay-statistics>

⁷¹ Following an inquiry by the European Commission, Apple committed to opening up access to the iPhone's NFC in the EU and a number of other countries. TechCrunch, “Apple opens up NFC transactions to developers, but says there will be ‘associated fees’”, 14 August 2024, <https://techcrunch.com/2024/08/14/apple-opens-up-nfc-transactions-to-developers-but-says-there-will-be-associated-fees>

⁷² 9To5Mac, “Brazil's antitrust watchdog says Apple must face penalties over NFC restrictions”, 1 July 2025, <https://9to5mac.com/2025/07/01/brazils-antitrust-watchdog-says-apple-must-face-penalties-over-nfc-restrictions/>

European Commission, “Antitrust: Commission seeks feedback on commitments offered by Apple over practices related to Apple Pay”, 19 January 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_282

⁷³ TechCrunch, “Apple's health offerings focus on data collection, not interpretation”, 3 June 2014, <https://techcrunch.com/2014/06/03/apples-health-offerings-focus-on-data-collection-not-interpretation>

⁷⁴ Apple Inc., HealthKit, <https://developer.apple.com/documentation/healthkit> (accessed 1 August 2025).

⁷⁵ Apple Inc., HealthKit (previously cited).

has led critics to argue that the company’s approach still consolidates vast amounts of sensitive information under its control – although it should be noted that Apple does not currently monetize health data through advertising.⁷⁶

⁷⁶ TechCrunch, “Apple’s health offerings focus on data collection, not interpretation” (previously cited).

3. HUMAN RIGHTS HARMS OF BIG TECH'S MARKET POWER

While the economic consequences of Big Tech's market dominance have received growing attention, the human rights harms linked to this power remain underexplored. This section sets out how monopolistic behaviour, anti-competitive practices, and even forms of market power that fall short of legal thresholds on monopolies can have far-reaching adverse implications for human rights. From undermining the right to privacy through exploitative data practices, to reinforcing structural discrimination via algorithmic bias, the consolidation of power in the hands of a few tech giants poses a series of risks to our rights.

3.1 EXCESSIVE DATA COLLECTION AND THE RIGHT TO PRIVACY

Traditional approaches to assessing market dominance have often focused on pricing power – a company's ability to raise prices above competitive levels – or practices such as price fixing. However, in the digital economy, dominance is increasingly exercised through the exploitation of data rather than just through price manipulation. Meta and Google's dominance of social media, search and online advertising is inextricably linked to their reliance on pervasive surveillance.⁷⁷ Meta and Google offer their core services for free but make money by harvesting and monetizing users' data at scale. Both companies, and many of the companies they own, depend on the large-scale collection of personal data to deliver curated content and targeted advertising.⁷⁸ This business model is not only fundamentally incompatible with the right to privacy;⁷⁹ it also reinforces their market power.

As outlined in section 2.1 "Google and Meta", the advertising infrastructure of these companies is embedded in millions of websites and across smartphones worldwide. This allows these companies to not only collect information we give them through using their websites, such as search queries, but also to gather personal and granular behavioural data, such as which application is in the foreground on your

⁷⁷ Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights* (previously cited).

⁷⁸ "We generate a significant proportion of our revenues from advertising" Alphabet Inc., *2024 Annual Report*, 31 January 2024, <https://abc.xyz/assets/70/a3/43ba8a804b49ac2fa2595c3c6704/2024-annual-report.pdf>; "We generate substantially all of our revenue from selling advertising placements on our family of apps to marketers" Meta Platforms, Inc., *2024 Annual Report*, 31 January 2025, <https://d18rnOp25nwr6d.cloudfront.net/CIK-0001326801/a8eb8302-b52c-4db5-964f-a2d796c05f4b.pdf>

⁷⁹ Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights* (previously cited).

smartphone.⁸⁰ The result is the construction of deeply intimate profiles about users that are then used to influence behaviour, primarily in order to make money by serving users targeted advertisements.^{81 82}

The data collected and used can be very personal. One striking example is the period and fertility tracking app Flo. In 2021, Flo was accused by the FTC of transmitting sensitive reproductive health data – including information about menstruation, ovulation and attempts to conceive – to third parties like Meta and Google via embedded software without explicit consent.⁸³ It was alleged that the transferred data could be used for any purpose including serving targeted advertisements, potentially exposing users to emotionally distressing content such as pregnancy-related ads after a miscarriage or infertility diagnosis. For these users the breach was deeply personal. Flo and the FTC reached a settlement in 2021 that required the app to obtain the affirmative consent of users before sharing their personal health data with others and to obtain an independent review of their privacy practices.⁸⁴

International human rights law stipulates that the right to privacy prohibits “arbitrary or unlawful interference” with an individual’s private life.⁸⁵ Such interference is only permissible under international human rights law if it is neither arbitrary nor unlawful – which means complying with principles of legality, necessity and proportionality.⁸⁶ The unprecedented scale and intrusiveness of Meta and Google’s data collection practices is inherently unnecessary and disproportionate given that the primary use of the data is for driving advertising profit, and is therefore not an acceptable interference with the right to privacy under international human rights law.⁸⁷

The right to privacy also includes the right to control how personal data is collected, used and shared. The rights to privacy and data protection are mutually reinforcing and interdependent. As affirmed in Article 1 of the Council of Europe’s Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108+), protecting personal data is not merely a matter of informational security, but a necessary condition for the enjoyment of privacy and other rights.⁸⁸

In a letter to Amnesty International on 25 August 2025, Meta stated that privacy is at the core of their company. However, while Google and Meta both provide tools for users to manage advert preferences, including the option to disable personalized advertisements altogether, these tools do not necessarily prevent data from being collected in the first place.⁸⁹ Personal and behavioural data may still be collected but used for other purposes such as personalizing content feeds or search query responses. In correspondence with Amnesty International Meta emphasized that they provide user tools for privacy protection. There are options – found in other parts of a users’ account settings – to disable *some* types of data collection such as location history.⁹⁰ However, while these tools are useful, they are complicated – users have to change a number of settings, in a number of different locations in order to restrict different types of data collection and to delete data already collected.⁹¹ It is so complicated that there are numerous online guides explaining how to delete your data and prevent Google and Meta from collecting it in future.⁹²

⁸⁰ Google, Privacy Policy (previously cited); Meta, Terms of Service, <https://www.facebook.com/legal/terms/update> (accessed on 1 August 2025).

⁸¹ Daron Acemoglu, Ali Makhdoumi, Azarakhsh Malekian, and Asuman Ozdaglar, “A model of behavioral manipulation”, 3 October 2023, <https://www.brookings.edu/articles/a-model-of-behavioral-manipulation/>; Lex Zard, “Consumer Manipulation via online behavioral advertising”, 30 December 2023, <https://arxiv.org/pdf/2401.00205>

⁸² Meta states that it handles data with special protections such as religious views provided by the user in accordance with national law and does not use it to serve advertisements. However, the Meta Privacy Policy also states that this information can still be used to “provide and improve” Meta Products. Meta Platforms, Inc., Privacy Policy, 26 July 2023, <https://mbasic.facebook.com/privacy/policy/printable/#annotation-30> (Your activity and information that you provide).

⁸³ Journal of High Technology Law, “Tracking trouble: The Flo health privacy scandal and what it means for your data”, 28 October 2024, <https://sites.suffolk.edu/jhtl/2024/10/28/tracking-trouble-the-flo-health-privacy-scandal-and-what-it-means-for-your-data>

⁸⁴ Federal Trade Commission, “FTC finalizes order with Flo Health, a fertility-tracking app that shared sensitive health data with Facebook, Google, and others”, 22 June 2021, <https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google>

⁸⁵ Universal Declaration of Human Rights (UDHR), Article 12; International Covenant on Civil and Political Rights (ICCPR), Article 17
⁸⁶ ICCPR, Article 17.

⁸⁷ Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights* (previously cited).

⁸⁸ Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).

⁸⁹ Google, Ad Center, https://myadcenter.google.com/personalizationoff?hl=en_US (accessed on 1 August 2025); Meta, Privacy Centre, <https://www.facebook.com/privacy/guide/ads> (accessed on 5 August 2025).

⁹⁰ Google, My Ad Center Help, <https://support.google.com/My-Ad-Center-Help/answer/12155964> (accessed on 1 August 2025), “Frequently asked questions”; Meta, Privacy Centre, <https://www.facebook.com/privacy/guide/collection> (accessed on 1 August 2025), “View and manage the info we’ve collected about you”

⁹¹ CNET, “There’s a way to delete the frightening amount of data Google has on you”, 31 January 2022, https://www.cnet.com/news/privacy/theres-a-way-to-delete-the-frightening-amount-of-data-google-has-on-you/#google_vignette

⁹² For example, Trusted Reviews, “How to stop Google collecting advertising data”, 14 March 2022, <https://www.trustedreviews.com/how-to/how-to-stop-google-collecting-advertising-data-4216921>; Consumer Reports, “Facebook privacy settings: How to make your account safer”, 28 January 2025, <https://www.consumerreports.org/electronics-computers/privacy/facebook-privacy-settings-a1775535782>

In 2022, human rights campaigner Tanya O’Carroll launched a legal case against Meta, alleging that the company had violated UK data protections laws.⁹³ While pregnant, before she had shared the news with her family, she noticed her Facebook feed was suddenly filled with baby-related adverts. She described the experience as “unnerving” as she had no way to opt out except to stop using Facebook and websites partnering with Facebook or using Meta tracking software altogether.⁹⁴ Her case highlights the deeply intrusive nature of surveillance-based targeted advertising, and the lack of meaningful control users have over how their data is used. In 2025, the case was settled prior to trial with Meta agreeing not to process O’Carroll’s data for direct marketing purposes.⁹⁵

Strategic acquisitions have also significantly expanded the data reach of Big Tech. Meta’s purchases of Instagram and WhatsApp, for example, not only prevented emerging platforms from being owned by rival companies but also expanded its surveillance reach across different modes of communication and social interaction. Google’s acquisitions of YouTube, Fitbit, and advertising technologies such as DoubleClick have enabled the company to consolidate vast datasets across video, health, and ad ecosystems. At the time of the Google–Fitbit merger in 2021, Amnesty International warned that the deal risked extending Google’s surveillance-based business model into the highly sensitive domain of health data.⁹⁶ Since then, the merger has gone ahead, and Google is now requiring Fitbit users to merge their Fitbit and Google accounts by February 2026 or risk losing access to their stored health and fitness data.⁹⁷

Meta and Google’s dominance in the digital economy is fundamentally rooted in their ability to collect, aggregate and monetize vast quantities of personal data. This data-driven market power has significant implications for the right to privacy, as individuals are systematically denied meaningful control over how their personal information is collected and used. The scale, intrusiveness and opacity of the surveillance-based business model is incompatible with international human rights standards, particularly the requirement that any interference with privacy be necessary, proportionate, and lawful. The data practices of Big Tech entrench their dominance in a self-reinforcing circle – the more data they collect, the more dominant they become, the more data they can collect, and so on – embedding a surveillance-based business model which is fundamentally incompatible with human rights.

3.2 IMPOSITION OF UNFAIR TERMS AND CONDITIONS

The market power of Big Tech companies has made it increasingly difficult to access the internet without interacting with their infrastructure or services – whether for search, video, e-commerce or social media. To use these services and infrastructure, users must accept the terms of service and privacy policies, many of which directly and negatively impact upon our rights.

Google’s UK privacy policy, effective 17 March 2025, outlines a broad range of data Google collects from users.⁹⁸ This includes information users actively provide (such as names and phone numbers), content users create or receive (such as emails and documents), location data and detailed information about the user’s activity online.⁹⁹ For Android users, the device also “periodically contacts Google servers to provide information about your device and connection to our services.... (including information such as) device type and carrier name, crash reports, which apps you’ve installed, and, depending on your device settings, other information about how you’re using your Android device”¹⁰⁰ Even users who are not logged into a Google account have data collected via unique identifiers tied to their browser, app or device.¹⁰¹

Similarly, users of Meta’s services (excluding Instagram, which has separate terms) must agree to Meta’s Terms of Service, which state: “You acknowledge that by using our Products, we will show you ads that we think may be relevant to you and your interests. We use your personal data to help determine which personalised ads to show you.”¹⁰² Meta’s privacy policy outlines that the company collects an expansive array of user-generated content, messages, metadata, purchase history, interactions with advertisements

⁹³ Brick Court Chambers, “Meta agrees not to process tech expert’s data for direct marketing purposes”, 25 March 2025, <https://www.brickcourt.co.uk/news/detail/meta-agrees-not-to-process-tech-experts-data-for-direct-marketing-purposes>

⁹⁴ BBC News, “Facebook to stop targeting ads at UK woman after legal fight”, 22 March 2025, <https://www.bbc.co.uk/news/articles/c1en1yiv4dpo>

⁹⁵ Brick Court Chambers, “Meta agrees not to process tech expert’s data for direct marketing purposes” (previously cited).

⁹⁶ Amnesty International, “EU Commission assessment of the Google–Fitbit merger must include human rights risks”, 27 November 2020, <https://www.amnesty.eu/news/eu-commission-assessment-of-the-google-fitbit-merger-must-include-human-rights-risks/>

⁹⁷ Android Central, “Fitbit warns about user data ahead of its 2026 Google account merge”, 28 March 2025, <https://www.androidcentral.com/wearables/fitbit/fitbit-google-account-merge-deadline-change-data-deletion>

⁹⁸ Google, Privacy Policy (previously cited).

⁹⁹ Google, Privacy Policy (previously cited).

¹⁰⁰ Google, Privacy Policy (previously cited).

¹⁰¹ Google, Privacy Policy (previously cited).

¹⁰² Meta, Terms of Service, (previously cited).

and AI tools, and information about contacts.¹⁰³ Meta gathers data about one specific user via other users too, for example, when someone uploads their address book or tags a person in a photo.¹⁰⁴ Meta also tracks user activity on smartphones, such as which app is in the foreground, and collects data shared through device settings, including GPS location, camera access and photos.¹⁰⁵ The company also receives information from third parties about websites visited, apps used and games played – allowing it to track users beyond its own platforms.¹⁰⁶

While in correspondence with Amnesty International Meta emphasized user privacy, both Google and Meta's terms of service and privacy policies are far-reaching. Google can read our private emails.¹⁰⁷ Meta and Google can track us across the internet. As a result, these companies often know where users live, work, who they live with, what they do for a living and even intimate details of their lives. This degree of data collection and use for advertising isn't, and can never be, compatible with our right to privacy (see section 3.1 "Excessive data collection and the right to privacy" for more details) but users are left with a restricted choice: accept terms that negatively impact our rights and gain access to Google and Meta's products and services, or don't accept them and be cut out from large swathes of the internet comprising crucial aspects of our personal and professional lives. Although it could be argued that it is technically possible – although incredibly difficult – for people to avoid using Google Search, YouTube, Facebook, Instagram and WhatsApp, the ubiquity of Google and Meta's advertising tracking technology across the web means that even if you avoid their direct products and services, it is virtually impossible to avoid them collecting at least some of your personal data.

Even in countries with legal protections which restrict the collection of sensitive data – such as the General Data Protection Regulation (GDPR) in the UK and EU – enforcing those rights in practice remains a major challenge. As demonstrated in the case of Tanya O'Carroll (see section 3.1 "Excessive data collection and the right to privacy" for more details), such legislation can be a powerful tool for protecting user rights. However, O'Carroll's case is just one example and it is yet to be seen if this important precedent will affect behavioural change at Meta.

Rights on paper do not always translate into meaningful accountability and protections. Enforcement is often slow, fragmented, and under-resourced, and fines are frequently absorbed as a cost of doing business. Meta, for example, has been served over €2.5 billion worth of fines under GDPR enforcement in the EU since 2019, Amazon €780 million and Google €215 million.¹⁰⁸ But these costs are dwarfed by their annual revenues (Meta \$164.50 billion,¹⁰⁹ Amazon \$637.96 billion,¹¹⁰ and Google \$350.02 billion¹¹¹). These penalties, while headline-grabbing, have done little to curb systemic rights violations by dominant platforms.

In 2023, Meta introduced a "pay or consent" model in the EU, offering users a choice between paying a subscription for an ad-free experience or consenting to data tracking for targeted advertising.¹¹² In July 2024, the European Commission issued preliminary findings that this model violated EU law. The Commission found that this consent model was not adequate, arguing that it did not give users a genuinely free choice.¹¹³ The European Data Protection Board (EDPB) has similarly stated that pay or consent models are unlikely to comply with the requirements for valid consent.¹¹⁴ The EDPB also states that obtaining consent does not absolve platforms of other data protection requirements such as necessity and proportionality.¹¹⁵ Ultimately, asking users to pay for privacy is not providing them with a free and fair choice.¹¹⁶

Regulators are increasingly recognizing the links between market power and unfair terms and conditions. For example, the Federal Competition and Consumer Protection Commission of Nigeria (FCCPC) found that

¹⁰³ Meta, Privacy Policy, <https://www.facebook.com/privacy/policy/?id=617> (accessed on 1 August 2025).

¹⁰⁴ Meta, Privacy Policy (previously cited).

¹⁰⁵ Meta, Terms of Service (previously cited).

¹⁰⁶ Meta, Terms of Service (previously cited).

¹⁰⁷ Google stopped using this data for ad targeting in 2017.

¹⁰⁸ GDPR Local, GDPR Enforcement Tracker, <https://gdprlocal.com/gdpr-enforcement-tracker> (accessed 25 July 2025).

¹⁰⁹ Stock Analysis, "Meta Platforms, Inc. (META) Revenue 2015–2025", <https://stockanalysis.com/stocks/meta/revenue> (accessed 1 August 2025).

¹¹⁰ Stock Analysis, "Amazon.com (AMZN) Revenue 2015–2025", <https://stockanalysis.com/stocks/amzn/revenue> (accessed 1 August 2025).

¹¹¹ Stock Analysis, "Alphabet (GOOGL) Revenue 2015–2025", <https://stockanalysis.com/stocks/googl/revenue> (accessed 1 August 2025).

¹¹² Tech Research Online, "Meta Faces EU Fines Over Controversial Pay-or-Consent Model", 27 June 2025, <https://techresearchonline.com/news/meta-pay-or-consent-eu-crackdown>

¹¹³ European Commission, "Commission sends preliminary findings to Meta over its 'Pay or Consent' model for breach of the Digital Markets Act", 1 July 2024, https://ec.europa.eu/commission/presscorner/detail/en/ip_24_358

¹¹⁴ European Data Protection Board, "Consent or Pay' models should offer real choice", 17 April 2024, https://www.edpb.europa.eu/news/news/2024/edpb-consent-or-pay-models-should-offer-real-choice_en

¹¹⁵ European Data Protection Board, "Consent or Pay' models should offer real choice" (previously cited).

¹¹⁶ European Digital Rights, "Privacy is not for sale: Meta must stop charging for people's right to privacy", 17 April 2024, <https://edri.org/our-work/privacy-is-not-for-sale-meta-must-stop-charging-for-peoples-right-to-privacy>

Meta abused its dominant position to push an exploitative change in WhatsApp's privacy policy on Nigerian consumers in January 2021.¹¹⁷ WhatsApp users in Nigeria were sent a message informing them that they must accept the new policy by 8 February to continue using the app.¹¹⁸ The regulator found that users were not given the option to withhold consent or determine how their data was used.¹¹⁹ In a novel move, the competition regulator in Nigeria worked closely with other authorities – including the data protection authority – allowing it to more easily assess the relationship between the abuse of market dominance and human rights impacts.¹²⁰

Another example of Big Tech imposing unfair terms and conditions is Meta's insistence in multiple lawsuits around the world that legal proceedings must be brought against it in California, USA, regardless of where harm has occurred, as per its terms of service. Courts such as the Supreme Court of Canada, have rejected this "forum selection clause", citing the stark imbalance of bargaining power between Facebook and its users.¹²¹ The Canadian court found that individuals are faced with little choice but to accept Facebook's terms of service.¹²² Though this "take it or leave approach" is used by many companies, users can in most cases simply choose not to use a service. But for companies like Meta, the ubiquity of its platforms makes agreeing to its terms of service more of a necessity for many users. This is because opting out of using platforms like Facebook, which is the predominant means of online communication and a key source of information in many countries (such as in Myanmar and Ethiopia – see section 3.3 "Amplification of harmful content" for more details), can put people at a social or informational disadvantage. The power dynamics are stark.

Companies like Meta seeking to use its terms of service to restrict the jurisdiction in which they can be sued can also create significant barriers for affected communities seeking remedy.¹²³ In one example, Abraham Meareg and Fisseha Tekle, together with The Katiba Institute, brought a case against Meta in Kenya alleging that the company played a role in amplifying harmful content during the armed conflict in northern Ethiopia (2020–2022).¹²⁴ Meta challenged the jurisdiction, arguing that its terms of service require all legal claims to be brought in US courts.¹²⁵ However, litigating in the US would require victims to navigate a foreign legal system and seek legal counsel in those countries – often in a different language, with unfamiliar procedures and prohibitive costs. These barriers make justice effectively inaccessible for many, especially those from conflict-affected or marginalized communities.¹²⁶ This practice undermines the right to an effective remedy, a cornerstone of international human rights law.

Big Tech's ability to dictate terms and conditions is particularly concerning in countries with limited regulatory oversight. In contexts with few legal protections, holding Big Tech to account for the human rights harm of their terms of service is even more difficult. Amnesty International's 2023 analysis of TikTok's privacy policy in the EU/UK/Switzerland, the US and Other Regions found significant disparities in privacy protections across jurisdictions.¹²⁷ For example, under the EEA/UK/Switzerland policy, TikTok needed to obtain user consent for the use of cookies where required by law.¹²⁸ This was not the case under the other two policies. Amnesty International also found that in some countries, TikTok did not collect precise or approximate GPS information but in "Other Regions" TikTok may collect precise location data (such as GPS) with a user's permission.¹²⁹ Ultimately, Amnesty found that TikTok's "Other Regions" policy allowed for the most extractive data practices of the three.¹³⁰ This differential treatment in some parts of the world is

¹¹⁷ TNP, "Examining the FCCPC's sanction of Meta Inc. for its alleged data privacy violation", 24 September 2024, <https://tnp.com.ng/insights/examining-the-fccpc-sanction-of-meta-inc-for-its-alleged-data-privacy-violation>

¹¹⁸ ARTICLE 19, "Nigerian Meta decision: the link between ensuring competition and protecting fundamental rights is a global issue", 27 August 2024, https://www.article19.org/wp-content/uploads/2024/08/Meta_Nigeria_Analysis_A19_Aug24.pdf

¹¹⁹ Nigerian Federal Competition & Consumer Protection Commission (FCCPC), *Investigative Report of the Federal Competition and Consumer Protection Commission and the Nigeria Data Protection Commission*, 13 November 2023, <https://fccpc.gov.ng/wp-content/uploads/2024/10/Investigative-Report-FCCPC-WhatsApp-13.11.23-1.pdf>

¹²⁰ FCCPC, *Investigative Report of the Federal Competition and Consumer Protection Commission and the Nigeria Data Protection Commission* (previously cited).

¹²¹ Supreme Court of Canada, *Douez v. Facebook, Inc.*, 2017 SCC 33, 23 June 2017, <https://www.canlii.org/en/ca/scc/doc/2017/2017scc33/2017scc33.html>

¹²² Supreme Court of Canada, *Douez v. Facebook, Inc.*, 2017 SCC 33 (previously cited).

¹²³ Amnesty International, "Meta can be sued in Kenya for role in Ethiopia conflict", 3 April 2025, <https://www.amnesty.org/en/latest/news/2025/04/kenya-high-court-has-ruled-that-it-has-jurisdiction-over-case-against-meta>

¹²⁴ Amnesty International, "Kenya: Meta sued for 1.6 billion USD for fuelling Ethiopia ethnic violence", 14 December 2022, <https://www.amnesty.org/en/latest/news/2022/12/kenya-meta-sued-for-1-6-billion-usd-for-fuelling-ethiopia-ethnic-violence>

¹²⁵ Amnesty International, "Meta can be sued in Kenya for role in Ethiopia conflict" (previously cited).

¹²⁶ Amnesty International, *Injustice Incorporated: Corporate Abuses and the Human Right to Remedy* (Index: POL 30/001/2014), 7 March 2014, <https://www.amnesty.org/en/documents/POL30/001/2014/en>

¹²⁷ Amnesty International, *'I Feel Exposed': Caught in TikTok's Surveillance Web* (Index: POL 40/7350/2023), 4 December 2023, <https://www.amnesty.org/en/documents/POL40/7349/2023/en>

¹²⁸ Amnesty International, *'I Feel Exposed': Caught in TikTok's Surveillance Web* (previously cited).

¹²⁹ Amnesty International, *'I Feel Exposed': Caught in TikTok's Surveillance Web* (previously cited).

¹³⁰ Amnesty International, *'I Feel Exposed': Caught in TikTok's Surveillance Web* (previously cited).

discriminatory and means that users in countries of the Global Majority are even more likely to be subject to unfair terms and conditions.

The imposition of unfair terms and conditions by powerful tech companies is a structural human rights issue. These terms have been shown to be exploitative, non-negotiable, and they disproportionately affect users in contexts with weaker regulatory protections. Even in jurisdictions with strong legal frameworks, enforcement is often too slow or too weak to meaningfully challenge the power of Big Tech. The result is a global digital environment where users are routinely denied meaningful consent and control over their rights.

3.3 AMPLIFICATION OF HARMFUL CONTENT

Several social media platforms have also been found to cause human rights harm by amplifying harmful content. Although the amplification of harmful content is not unique to Meta, its global dominance in social media has not only magnified the reach of its platforms but also the scale of harm caused by its algorithmic amplification of inflammatory content on those platforms – with devastating human rights consequences. This is clear in Myanmar and Ethiopia, where Facebook became a vector for incitement, discrimination and violence against marginalized communities.

Meta’s surveillance-based business model relies on maximizing user engagement to collect personal data and serve targeted advertisements. To achieve this, Meta has designed its recommender systems – content-ranking and recommender algorithms – to prioritize content likely to provoke strong emotional reactions, such as outrage or fear, because such content has been shown to keep users online longer.¹³¹ Meta denies that its News Feed algorithm is designed to maximize engagement, stating that “the actual goal is to connect people with the content that is most interesting and relevant to them.”¹³² In its written response to Amnesty International’s allegations, the company highlighted that it provides certain tools across its platforms so that users can manage the types of content they see.¹³³ However, it remains true that the longer users remain on the platform, the more data Meta can extract and advertising revenue it can generate.

Amnesty’s investigations into Facebook’s role in the ethnic cleansing of the Rohingya in Myanmar (2017) and the Tigray war in Ethiopia (2020 – 2022), found that Facebook’s algorithms “supercharged” the spread of harmful rhetoric targeting these communities.¹³⁴ In both cases, Facebook not only failed to effectively moderate such harmful content but actively amplified it, contributing to serious human rights violations.¹³⁵

In both Myanmar and Ethiopia, Facebook played an extremely important role in the information ecosystem. In Myanmar, Facebook was not just a social media platform – it was described as “the internet” for many people during 2017 as the platform was so deeply embedded in the country’s communication infrastructure.¹³⁶ Access to “Free Basics”, a service that provided users with access to a basic version of Facebook along with a limited number of services without incurring data charges on their mobile phones, and “Facebook Flex”, a product that enables subscribers to have a text-only version of Facebook without incurring data charges, made Facebook the most affordable and accessible online platform.¹³⁷ Facebook became the primary news source, business directory, online marketplace and go-to search engine.¹³⁸ Even government announcements were often made through Facebook.¹³⁹

The platform’s dominance in Myanmar, combined with low digital literacy and limited access to alternative information, created a perfect storm. In the lead-up to and during the 2017 atrocities against the Rohingya, Facebook became a megaphone for hate. Military officials and nationalist groups used the platform to spread

¹³¹ Amnesty International, *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>

¹³² Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights* (previously cited), annex

¹³³ To read more about these tools please see Meta’s response to Amnesty International available in the annex to this briefing.

¹³⁴ Amnesty International, *The Social Atrocity: Meta and the Right to Remedy for the Rohingya* (previously cited); 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>;

Amnesty International wrote to Meta on 20 May 2022 and asked what measures the company took prior to 2017 to prevent its algorithmic systems from being used to amplify advocacy of hatred against the Rohingya. Meta responded that “Meta’s investments in Myanmar in response to the events in 2017 have been significant” but added that that the company could not provide information concerning the period leading up to 2017 because the company is “currently engaged in litigation proceedings in relation to related matters”.

¹³⁵ Amnesty International, *The Social Atrocity: Meta and the Right to Remedy for the Rohingya* (previously cited); Amnesty International, ‘A Death Sentence for My Father’: *Meta’s Contribution to Human Rights Abuses in Northern Ethiopia* (previously cited).

¹³⁶ Amnesty International, *The Social Atrocity: Meta and the Right to Remedy for the Rohingya* (previously cited).

¹³⁷ Independent International Fact-Finding Mission on Myanmar, *Report of the Detailed Findings of the Independent International Fact-Finding Mission on Myanmar* (IIFMM, Detailed findings), 17 September 2018, A/HRC/39/CRP.2 para. 1344.

¹³⁸ IIFMM, *Detailed findings*, (previously cited), para. 1345.

¹³⁹ IIFMM, *Detailed findings*, (previously cited), para. 1345.

dehumanizing rhetoric, portraying the Rohingya as “invaders” and “vermin.”¹⁴⁰ Posts inciting violence – some calling for the extermination of the Rohingya – were algorithmically amplified and widely shared.¹⁴¹ Despite repeated warnings from civil society and UN experts, Meta failed to act and ultimately contributed to the ethnic cleansing suffered by the Rohingya.¹⁴²

In Ethiopia, Facebook was similarly the dominant platform for news and political discourse. Internet access expanded rapidly during the 2010s and Facebook quickly became the most widely used social media platform in the country, with many internet users using it as a news source, and to share information and opinions.¹⁴³ During the Tigray conflict (2020–2022), Meta’s algorithms amplified content that incited hatred and violence against Tigrayans. Government officials and pro-government activists used Facebook to dehumanize the entire ethnic group. For example, Prime Minister Abiy Ahmed posted in July 2021 calling Tigray forces “weeds” and a “cancer”.¹⁴⁴ These narratives were not only tolerated but boosted by Meta’s systems.¹⁴⁵ The consequences were deadly. In one case, Professor Meareg Amare, a Tigrayan academic, was murdered after being targeted in Facebook posts that revealed his identity and location. His son, Abraham, reported the posts to Meta but they remained online until after his father’s death.¹⁴⁶ Meta sent a letter to Amnesty International on 25 October 2023 stating that they ‘fundamentally disagreed’ with these allegations, and stated that Ethiopia is a priority country for intervention, further noting that Meta was unable to respond more fully due to pending litigation.¹⁴⁷

The conflation of Facebook with the internet is not unique to Myanmar and Ethiopia. Outside of China – which has its own social media platforms – Facebook’s dominance of social media networking means people in many countries are increasingly getting their news and engaging in public discourse through the platform. In the US, the FTC recently brought a major antitrust lawsuit alleging that Meta, through its Facebook and Instagram platforms, has maintained an illegal monopoly in social media.¹⁴⁸ The FTC notes that no other platform in the US comes close to matching Facebook or Instagram’s scale.¹⁴⁹

The dominance of social media platforms in conflict-affected zones and their role during crises is particularly concerning. When a single platform functions as the “front page of the internet”, the amplification of harmful content, and the failure to effectively moderate it, can have especially harmful consequences. In such contexts, users are less likely to encounter alternative sources of information that might counterbalance or contextualize inflammatory rhetoric and are therefore more likely to believe it.¹⁵⁰

In Myanmar in 2017, Facebook was widely perceived as a reliable source of news and information as a US-based platform populated by trusted friends and family.¹⁵¹ The Independent International Fact-Finding Mission on Myanmar observed that “the Government’s use of Facebook for official announcements and sharing of information further contributes to users’ perception of Facebook as a reliable source of information”.¹⁵² Meta’s contribution to the ethnic cleansing of the Rohingya was substantial in nature because the core features of the Facebook platform (specifically its news feed, ranking, and recommendation algorithms) actively amplified, promoted and delivered posts inciting advocacy of hatred and violence against the Rohingya to target audiences who were most likely to act upon them.¹⁵³ The effects of these actions for the Rohingya were especially severe because of the near-total dominance of the Facebook platform within Myanmar’s online environment at the time.

In 2023, Amnesty International found that TikTok’s algorithmic recommender system exposed children and young people to serious health risks, by exploiting psychological vulnerabilities to maximize their engagement

¹⁴⁰ Amnesty International, *The Social Atrocity: Meta and the Right to Remedy for the Rohingya* (previously cited).

¹⁴¹ Amnesty International, *The Social Atrocity: Meta and the Right to Remedy for the Rohingya* (previously cited).

¹⁴² Amnesty International, *The Social Atrocity: Meta and the Right to Remedy for the Rohingya* (previously cited).

¹⁴³ Iginio Gagliardone, et al., “Mechachal: Online debates and elections in Ethiopia. From hate speech to social engagement on social media”, 2016, <https://ora.ox.ac.uk/objects/uuid:da10c4ee-2726-41cf-ba21-72c9f7cbc440>

¹⁴⁴ Amnesty International, ‘A Death Sentence for My Father’: Meta’s Contribution to Human Rights Abuses in Northern Ethiopia (previously cited).

¹⁴⁵ Amnesty International, ‘A Death Sentence for My Father’: Meta’s Contribution to Human Rights Abuses in Northern Ethiopia (previously cited).

¹⁴⁶ Amnesty International, ‘A Death Sentence for My Father’: Meta’s Contribution to Human Rights Abuses in Northern Ethiopia (previously cited).

¹⁴⁷ To read Meta’s response please see Amnesty International, ‘A Death Sentence for My Father’: Meta’s Contribution to Human Rights Abuses in Northern Ethiopia (previously cited) annex.

¹⁴⁸ Federal Trade Commission, *Facebook, Inc., FTC v. (FTC v. Meta Platforms, Inc.)*, 15 April 2025, <https://www.ftc.gov/legal-library/browse/cases-proceedings/191-0134-facebook-inc-ftc-v-ftc-v-meta-platforms-inc>

¹⁴⁹ Federal Trade Commission, *Facebook, Inc., FTC v. (FTC v. Meta Platforms, Inc.)* (previously cited).

¹⁵⁰ Eva Surawy Stepney and Clare Lally, “Disinformation: sources, spread and impact”, 25 April 2024, <https://researchbriefings.files.parliament.uk/documents/POST-PN-0719/POST-PN-0719.pdf>; American Psychological Association, “What psychological factors make people susceptible to believe and act on misinformation?”, 1 March 2024, <https://www.apa.org/topics/journalism-facts/misinformation-belief-action>

¹⁵¹ IFFMM, *Detailed findings*, (previously cited).

¹⁵² IFFMM, *Detailed findings*, (previously cited).

¹⁵³ Amnesty International, *The Social Atrocity: Meta and the Right to Remedy for the Rohingya* (previously cited).

with the platform and profit for the company. Amnesty International's report *Driven into Darkness* documented how young users showing an interest in mental health-related video content could be drawn into harmful rabbit holes, including content that romanticized, normalized or encouraged self-harm and suicide, within 20 minutes of signing up to the platform. In promoting such content, TikTok risked exposing a child or young person experiencing depressive symptoms to a harmful social media feed, which had the potential to exacerbate pre-existing mental health issues and could potentially contribute to devastating real-world actions.¹⁵⁴ Although TikTok is not one of the "Big 5" tech companies which are the focus of this briefing, the company's rapid growth in recent years suggests it could become comparably dominant within the social media sector in future.

Amnesty International has repeatedly documented how social media platforms – such as Facebook, X and TikTok – can contribute to serious human rights violations by failing to effectively moderate, and by actively amplifying, harmful content.¹⁵⁵ Addressing the harms of algorithmic amplification will require tackling market power as a key part of the solution, since part of the issue is scale and market dominance over information access. However, structural solutions such as breaking up social media companies would not be sufficient on their own. Governments must pair these structural measures with behavioural requirements – such as disabling personalized feeds by default – to fully address the human risks posed by amplification.

3.4 FREEDOM OF EXPRESSION, OPINION AND ACCESS TO INFORMATION

The combination of Google and Meta's significant market power and their ability to personalize content means these platforms play a substantial role in shaping people's online experience and determining the information we see. These factors also mean that these companies have an outsized influence over shaping public opinion – all while being incentivised to maximize corporate profits, even at the expense of public safety and human rights. The dominance of these companies in the digital ecosystem therefore could, and in some cases has already, have profound implications for freedom of opinion and expression and the right to access information.

The rights to freedom of opinion, freedom of expression, and access to information are deeply interdependent and mutually reinforcing. Freedom of opinion – considered an absolute right and enshrined under article 18 of the Universal Declaration of Human Rights and article 18 of the International Covenant on Civil and Political Rights – protects the right to hold views without interference or manipulation.¹⁵⁶ Freedom of expression enables individuals to communicate those opinions and ideas to others. Crucially, the right to seek and receive information is an essential component of freedom of expression, as individuals must have access to diverse and reliable information in order to form opinions and participate meaningfully in public discourse. Under international human rights law, the right to freedom of expression and access to information are protected by Article 19 of the International Covenant on Civil and Political Rights, which guarantees the right to "freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds."¹⁵⁷ These rights are inextricably linked and apply in both online and offline environments.¹⁵⁸ When a small number of companies control the primary gateways to information, their decisions can have systemic effects on the public's ability to access diverse viewpoints and thus on access to information, freedom of opinion and expression.

Use of Meta's social platforms and Google's search and YouTube have become so embedded in the fabric of the internet that meaningful participation in online life often depends on using their platforms. The proportion of people who use Facebook, Instagram and/or YouTube is extremely high. Even for users who don't regularly post on these sites, many get information through these platforms, including news. In April 2025, it was reported that 91.5% of internet users accessed online video and 88.4% accessed social media

¹⁵⁴ To see the full details of Amnesty International's research as well as TikTok's response please see: Amnesty International, *Driven into Darkness: How TikTok's 'For You' Feed Encourages Self-Harm and Suicidal Ideation* (Index: POL 40/7350/2023), 7 November 2023, <https://www.amnesty.org/en/documents/POL40/7350/2023/en>

¹⁵⁵ Amnesty International, *The Social Atrocity: Meta and the Right to Remedy for the Rohingya* (previously cited); Amnesty International, *'A Death Sentence for My Father': Meta's Contribution to Human Rights Abuses in Northern Ethiopia* (previously cited); Amnesty International, *Driven into Darkness: How TikTok's 'For You' Feed Encourages Self-Harm and Suicidal Ideation* (previously cited); Amnesty International, *Technical Explainer on X's Recommender System and the 2024 Racist Riots* (Index: EUR 45/0618/2025), 6 August 2025, <https://www.amnesty.org/en/documents/eur45/0618/2025/en>

¹⁵⁶ UDHR, Article 18; ICCPR, Article 18.

¹⁵⁷ ICCPR, Article 19.

¹⁵⁸ UN Human Rights Council (UNHRC), Resolution 57/29: *Promotion, protection and enjoyment of human rights on the Internet*, adopted on 11 October 2024, UN Doc. A/HRC/RES/57/29.

weekly.¹⁵⁹ Internet users spent a weekly average of 11 hours and 34 minutes on online video and 7 hours and 8 minutes on social media.¹⁶⁰ Google, YouTube, Facebook, Instagram and X were the most visited websites on the web between December 2024 and February 2025.¹⁶¹ Google also reportedly claimed 90.15% of all search engine referrals¹⁶² and Google Chrome held 67.48% of global browser market share.¹⁶³

The Cambridge Analytica scandal exemplified how the unchecked power of dominant digital platforms can undermine freedom of opinion, expression, and access to information. In 2018, it was revealed that Cambridge Analytica harvested personal data from up to 87 million Facebook users without consent, using a personality quiz app to build psychographic profiles for targeting of political messaging.¹⁶⁴ Whistleblowers accused Cambridge Analytica of weaponizing this data to influence electoral outcomes, including the 2016 US presidential election and the Brexit referendum.¹⁶⁵ Facebook was fined \$5 billion by the FTC and £500,000 by the UK's data protection watchdog for its role in the Cambridge Analytica scandal.¹⁶⁶ In 2018, Facebook demanded that Cambridge Analytica delete the data.¹⁶⁷

Across their platforms, these companies have immense power over what information people see and, through their content moderation policies, what is allowed to remain on their sites. When Elon Musk took over in 2022, Twitter's (now X) content moderation policies were changed to remove the prohibition of "misgendering or deadnaming" transgender individuals. Policies on "crisis misinformation", "COVID-19 misleading information" and "misinformation about election outcomes" were also removed.¹⁶⁸ In January 2025, around the same time as the second inauguration of Donald Trump as US president, Meta announced changes to content policies on its platforms to "allow more speech".¹⁶⁹ The policies now allowed, for example, "allegations of mental illness or abnormality when based on gender or sexual orientation" while a section which banned users from targeting people "with claims that they have or spread the novel coronavirus" was removed.¹⁷⁰ A section banning referring to women "as household objects or property or objects in general" and calling transgender or non-binary people "it" was also removed.¹⁷¹

However, it is not just content moderation policies that impact what speech remains on these platforms, but also how those policies are implemented. After Musk became CEO, X dissolved its trust and safety council – an advisory group of around 100 independent civil society organizations formed to help address topics such as hate speech – and slashed the size of the content moderation and trust and safety teams.¹⁷² Without adequate content moderation and trust and safety teams, the risk that policies are inconsistently applied increases.

Some social media platforms have also been seen to invest less in risk mitigation and content moderation in countries of the Global Majority. During the 2017 ethnic cleansing of Rohingya Muslims in Myanmar (see section 3.3 "Amplification of harmful content" for more details), Facebook had just one Burmese-speaking content moderator.¹⁷³ Facebook has since stated that it has hired additional content moderators in Burmese but in 2017 the company's responses to content moderation reports were found to be "slow and ineffective".¹⁷⁴ Several activists told Amnesty International that they had repeatedly reported content that violated Facebook's policies. Sharif, a 28-year-old Rohingya community educator, told Amnesty International that he reported anti-Rohingya content "more than 100 times" since 2014, and no action was ever taken.¹⁷⁵

¹⁵⁹ DataReportal, *Digital 2025 April Global Statshot Report*, 23 April 2025, <https://datareportal.com/reports/digital-2025-april-global-statshot>

¹⁶⁰ DataReportal, *Digital 2025 April Global Statshot Report* (previously cited).

¹⁶¹ DataReportal, *Digital 2025 April Global Statshot Report* (previously cited).

¹⁶² DataReportal, *Digital 2025 April Global Statshot Report* (previously cited).

¹⁶³ Oberlo, "Most popular web browsers in 2024", December 2024, <https://www.oberlo.com/statistics/browser-market-share> (accessed 1 August 2025).

¹⁶⁴ BBC News, "Facebook fined £500,000 for Cambridge Analytica scandal", 25 October 2018, <https://www.bbc.co.uk/news/technology-45976300>

¹⁶⁵ Politico, "Cambridge Analytica helped 'cheat' Brexit vote and US election, claims whistleblower", 27 March 2018, <https://www.politico.eu/article/cambridge-analytica-chris-wylie-brexit-trump-britain-data-protection-privacy-facebook>

¹⁶⁶ BBC News, "Facebook fined £500,000 for Cambridge Analytica scandal" (previously cited); Federal Trade Commission, "FTC imposes \$5 billion penalty and sweeping new privacy restrictions on Facebook", 24 July 2019, <https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook>

¹⁶⁷ Facebook, "Hard Questions: Update on Cambridge Analytica", 21 March 2018, <https://newsroom.fb.com/news/2018/03/hard-questions-cambridge-analytica>

¹⁶⁸ Adrian Kopps, "Two years after the takeover: Four key policy changes of X under Musk", 28 October 2024, <https://zenodo.org/records/14040407>

¹⁶⁹ Meta, Transparency Center, <https://transparency.meta.com/en-gb/features/how-fact-checking-works> (accessed 25 July 2025), "How fact-checking works"

¹⁷⁰ Meta, "How fact-checking works" Transparency Center (previously cited).

¹⁷¹ Meta, "How fact-checking works" Transparency Center (previously cited).

¹⁷² Associated Press, "Musk's Twitter disbands its Trust and Safety advisory group", 13 December 2022, <https://apnews.com/article/elon-musk-twitter-inc-technology-business-a9b795e8050de12319b82b5dd7118cd7>

¹⁷³ Referenced in Cecilia Kang and Sheera Frenkel, *An Ugly Truth: Inside Facebook's Battle for Domination*, and confirmed by an Amnesty International interview with activist who was in the Facebook group (evidence on file with Amnesty International).

¹⁷⁴ IFFMM, *Detailed findings* (previously cited).

¹⁷⁵ Amnesty International interview with Mohamed Sharif (pseudonym), 13 April 2022 (evidence on file with Amnesty International).

Showkutara had a similar experience, and recalled her dismay at Meta's repeated failure to act in response to her reports:

"There were so many pages and contents, how could I report them all? I was not able to do anything against all these things. But I did report some, and I just received a message [that no action would be taken]... I really wanted to stop these things on Facebook, and I tried a lot – I just cried when I saw this, I didn't have any other option. I really wanted Facebook to stop this hate speech spreading, but I could not, and it made me so upset."¹⁷⁶

Most reports of violating content either went ignored or were incorrectly determined to have not violated Facebook's community standards.¹⁷⁷

As well as shaping content through policies and content moderation implementation, social media platforms and search engines like Facebook and Google shape what users see and when through algorithmic recommender systems. Algorithmic recommender systems are now "a critical part of the information environment,"¹⁷⁸ embedded in search engines, social media, and content platforms. These systems filter and prioritize content, shaping what users see and potentially even limiting exposure to diverse viewpoints. The opacity of these recommender systems, as well as our lack of control over them, means that we are often passively served content that may shape our opinions and values without a means to control or change what we see. As stated by the UN Special Rapporteur on the promotion and protection of the right to freedom of expression, "the artificial intelligence applications for search have enormous influence over the dissemination of knowledge. Content aggregators and news sites... choose which information to display to an individual based not on recent or important developments, but on artificial intelligence applications that predict users' interests and news patterns based on extensive datasets. Consequently, artificial intelligence plays a large but usually hidden role in shaping what information individuals consume or even know to consume."¹⁷⁹

Ultimately, search and social media platforms have the ability to subtly shape public discourse by tweaking what is promoted or suppressed, either knowingly through inputting certain parameters or through algorithmic bias. Amnesty International research has repeatedly shown that recommender systems used by social media platforms are not neutral.¹⁸⁰ Programmed to keep us on these platforms for longer, algorithmic recommender systems often appeal to emotions that increase engagement such as outrage or fear. For instance, a technical investigation conducted by Amnesty International, the Algorithmic Transparency Institute (National Conference on Citizenship) and AI Forensics in 2023 showed that children and young people who watched mental health-related content on TikTok's "For You" feed could easily be drawn into "rabbit holes" of potentially harmful content, including videos that romanticized and encouraged depressive thinking, self-harm and suicide.¹⁸¹

Research also suggests that users of social media platforms initially start with a broad range of views but gradually polarize toward ideological extremes.¹⁸² Algorithmically recommended content can help contribute to this effect as users are served more and more content they agree with and are likely to engage with, and are therefore drawn further into rabbit holes of similar content.¹⁸³ These information silos lead to echo chambers as users are more likely to be repeatedly shown content that aligns with their views, reinforcing existing beliefs. Repeated exposure to algorithmic biases can shape and manipulate users' beliefs without their knowledge.

¹⁷⁶ Amnesty International interview by video call with Showkutara, 06 April 2022 (evidence on file with Amnesty International).

¹⁷⁷ Amnesty International, *The Social Atrocity: Meta and the Right to Remedy for the Rohingya* (previously cited).

¹⁷⁸ UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Promotion and Protection of Human Rights: Human Rights Questions, Including Alternative Approaches for Improving the Effective Enjoyment of Human Rights and Fundamental Freedoms*, 29 August 2019, UN Doc. A/73/348.

¹⁷⁹ David Kaye, UN Special Rapporteur on the Promotion and protection of the right to freedom of opinion and expression report to the UN General Assembly, 29 August 2018, A/73/348, para.24.

¹⁸⁰ Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights* (previously cited); Amnesty International, *The Social Atrocity: Meta and the Right to Remedy for the Rohingya* (previously cited); Amnesty International, *'A Death Sentence for My Father': Meta's Contribution to Human Rights Abuses in Northern Ethiopia* (previously cited).

¹⁸¹ Amnesty International, *Driven into Darkness: How TikTok's 'For You' Feed Encourages Self-Harm and Suicidal Ideation* (previously cited).

¹⁸² Mohammed Shahid Modi, James Flamino and Boleslaw K. Szymanski, "Dynamics of ideological biases of social media users", 1 May 2024, IEEE Communications Magazine, Volume 62, Issue 5, pp. 36–42, <https://ieeexplore.ieee.org/document/10520172>; Chen Avin, Hadassa Daltrophe and Zvi Lotker, "On the impossibility of breaking the echo chamber effect in social media using regulation", 11 January 2024, Scientific Reports, Volume 14, 1107, <https://www.nature.com/articles/s41598-023-50850-6#citeas>

¹⁸³ Derek O'Callaghan, Derek Greene, Maura Conway, Joe Carthy and Pádraig Cunningham, "Down the (white) rabbit hole: The extreme right and online recommender systems", 16 October 2014, Social Science Computer Review, Volume 33, Issue 4, pp. 459–478, <https://doi.org/10.1177/089443931455553>; "On Facebook and Twitter... users with a given leaning are much more likely to be reached by information propagated by users with similar leaning" Matteo Cinelli, Gianmarco De Francisci Morales, Alessandro Galeazzi, Walter Quattrociocchi and Michele Starnini, "The echo chamber effect on social media", 2 March 2021, Proceedings of the National Academy of Sciences of the United States of America, Volume 118, Issue 9, <https://doi.org/10.1073/pnas.2023301118>; Amnesty International, *Driven into Darkness: How TikTok's 'For You' Feed Encourages Self-Harm and Suicidal Ideation* (previously cited).

Google and Meta’s market power in the digital ecosystem – combined with their ability to personalize, curate, and moderate content – grants them extraordinary power over the flow of information and the boundaries of public discourse. As the UN Special Rapporteur on freedom of expression has warned, algorithmic systems used in search and content delivery now play a hidden but decisive role in shaping what individuals know, believe, and are exposed to.¹⁸⁴ This opaque influence undermines our access to information – a cornerstone of international human rights law. Urgent interventions are needed to disrupt the influence of a small number of companies over online public discourse.

3.5 CROWDING OUT THE POTENTIAL FOR RIGHTS-RESPECTING ALTERNATIVES

Google has been accused of holding five different monopolies: search,¹⁸⁵ advertising technology,¹⁸⁶ browsers,¹⁸⁷ smartphone operating system¹⁸⁸ and app distribution.¹⁸⁹ Meta has been accused of illegally maintaining a monopoly in personal social networking.¹⁹⁰ Although several of these cases are yet to be decided, it is evident that Google and Meta’s market power in each of these areas has been achieved in large part through strategic acquisitions.

Google’s purchases of DoubleClick (2008), Invite Media (2010) and AdMeld (2011) allowed the company to maintain and reinforce its market share in the online advertising market by acquiring companies that control different parts of the advertising process (vertical acquisitions). As well as giving Google control over the full “ad stack”, Google has been accused of buying up potential competitors to maintain its control of the advertising technology space.¹⁹¹

Android’s global market share of smartphone operating systems – which currently stands at 72% – has been at least 65% for the last decade.¹⁹² It is even higher in Africa and South America, where Android’s market share currently stands at over 85%.¹⁹³ By preinstalling Google Chrome and other Google apps onto Android smartphones Google has strategically used its dominance in one area – smartphone operating systems – to support its dominance in others – browsers and search.¹⁹⁴ This move coupled with the dominance of Android has entrenched pervasive data collection on smartphone devices – and near constant surveillance of smartphone users.

Meta’s acquisition of Instagram (2012) and WhatsApp (2014) have similarly come under scrutiny, with the FTC accusing Meta of illegally buying or burying competitors (horizontal acquisitions) when Meta failed to successfully thrive during the transition to mobile.¹⁹⁵ Furthermore, the FTC states that “Facebook’s actions have suppressed innovation and product quality improvement... degrading the social network experience (and) subjecting users to lower levels of privacy and data protections and more intrusive ads.”¹⁹⁶

¹⁸⁴ UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, *Promotion and Protection of Human Rights: Human Rights Questions, Including Alternative Approaches for Improving the Effective Enjoyment of Human Rights and Fundamental Freedoms* (previously cited).

¹⁸⁵ The Verge, “Judge rules on US DOJ v. Google antitrust search suit”, 5 August 2024, <https://www.theverge.com/2024/8/5/24155520/judge-rules-on-us-doj-v-google-antitrust-search-suit>

¹⁸⁶ US Department of Justice, “Department of Justice prevails in landmark antitrust case against Google”, 17 April 2025, <https://www.justice.gov/opa/pr/departments-justice-prevails-landmark-antitrust-case-against-google>

¹⁸⁷ The Verge, “DOJ pushes for Google to break off Chrome browser after antitrust case”, 21 November 2024, <https://www.theverge.com/2024/11/20/24300617/doj-google-search-antitrust-chrome-breakup>

¹⁸⁸ David Bassali, Adam Kinkley, Katie Ning and Jackson Skeen, *Google’s Anticompetitive Practices in Mobile: Creating Monopolies to Sustain a Monopoly*, May 2020, Thurman Arnold Project, Yale School of Management, <https://som.yale.edu/sites/default/files/2022-01/DTH-GoogleMobile.pdf>

¹⁸⁹ PCMag UK, “Google Play Store is a monopoly, jury finds”, 12 December 2023, <https://uk.pcmag.com/mobile-apps/150086/google-play-store-is-a-monopoly-jury-finds>

¹⁹⁰ Federal Trade Commission, “FTC alleges Facebook resorted to illegal buy-or-bury scheme to crush competition after string of failed attempts to innovate”, 19 August 2021, <https://www.ftc.gov/news-events/news/press-releases/2021/08/ftc-alleges-facebook-resorted-illegal-buy-or-bury-scheme-crush-competition-after-string-failed>

¹⁹¹ Business Standard, “US Justice Dept says Google saw ad startup AdMeld as threat and bought it”, 17 September 2024, https://www.business-standard.com/world-news/us-justice-dept-says-google-saw-ad-startup-admeld-as-threat-and-bought-it-124091700128_1.html

¹⁹² SOAX, “What’s Android Market Share?”, 9 January 2025, <https://soax.com/research/android-market-share> (accessed on 29 July 2025).

¹⁹³ SOAX, “What’s Android Market Share?” (previously cited).

¹⁹⁴ DeviceMAG, “The Complete List of Pre-Installed Apps on Android Devices”, 22 December 2023, <https://www.devicemag.com/android-pre-installed-apps-list/> (accessed on 1 August 2025).

¹⁹⁵ Federal Trade Commission, “FTC alleges Facebook resorted to illegal buy-or-bury scheme to crush competition after string of failed attempts to innovate” (previously cited).

¹⁹⁶ Federal Trade Commission, “FTC alleges Facebook resorted to illegal buy-or-bury scheme to crush competition after string of failed attempts to innovate” (previously cited).

As outlined in section 2.1 “Meta and Google”, Meta’s social media platforms have also benefited from network effects – where a product or service becomes more valuable to its users as more people use it. Network effects can make it difficult for new competitors to break through.¹⁹⁷ Meta has maintained its dominant position in social networking by creating significant barriers to switching platforms and therefore locking in users they gathered through network effects. Users who have built up connections and have a history of posts and photos on Meta’s platforms cannot easily transfer that information to another network and thus may be less likely to leave.

Ultimately, the strategy of buying out competition before it can mature has stifled innovation, reduced consumer choice and concentrated control over the digital public sphere into the hands of just a few actors. This stifling of competition has entrenched the surveillance-based business model of Meta and Google as the central business model of the internet, but it doesn’t have to be this way. The potential for alternatives that do respect our rights have ultimately been squashed, and business models that are inherently anti-rights have become normalized.

Network effects have further locked in users to a small number of platforms. One option open to regulators is to require dominant services to open up through interoperability mandates – rules that require dominant platforms to allow their services to integrate with other platforms. Interoperability would mean that users could choose alternative platforms without losing the ability to communicate with their friends and family, much like how email works across different providers (in other words, someone with a Gmail address can correspond with someone who has an Outlook address – in contrast to how social media platforms operate). This would give people more meaningful choices about where and how they engage online.

3.6 LABOUR RIGHTS ABUSES

The sheer economic scale of Big Tech and the workforce required to deliver its functions and products, has allowed it to have a significant influence on global labour practices. For example, Amazon’s global market dominance in e-commerce has enabled it to dictate labour conditions across its operations and supply chains in ways that often undermine workers’ rights. To maintain its competitive edge and profit margins (and therefore market dominance), Amazon has relentlessly driven down costs both in its own operations and those of its suppliers and contractors.¹⁹⁸ Amazon’s significant power in online retail – serving more than 310 million active users globally¹⁹⁹ – has allowed it to impose increasingly extractive terms on sellers and contractors, including rising fees for logistics and advertising services.²⁰⁰ These costs are passed down the chain, squeezing margins and creating pressure to cut costs elsewhere, including labour costs.

This dynamic is replicated globally, including in high-risk human rights environments like Saudi Arabia, where Amnesty International has documented serious abuses of migrant workers contracted to Amazon.²⁰¹ Amnesty International research from 2023 found that Amazon’s reliance on third-party labour supply companies in Saudi Arabia enabled it to benefit from a flexible, low-cost workforce while distancing itself from direct accountability for serious human rights abuses.²⁰² Migrant workers from Nepal were deceived by recruitment agents about the nature of the employment, cheated of promised pay and benefits, punished if they complained and housed in squalid conditions by third-party contractors. Amnesty concluded that the severity and deceptive nature of the treatment likely constituted human trafficking for labour exploitation under international law.²⁰³

Amnesty also found that workers were compelled to meet gruelling productivity targets in Amazon-run warehouses, often under surveillance and without adequate rest, echoing concerns raised in other jurisdictions about Amazon’s use of algorithmic management and performance pressure. Workers were also then abandoned by the labour supply companies without pay or support once their engagement in Amazon warehouses ended. These abuses were not isolated incidents but stemmed from systemic failures in Amazon’s human rights due diligence and a business model that prioritizes operational flexibility and cost

¹⁹⁷ US Federal Trade Commission, *Administrative Part 3 Complaint: Meta Platforms, Inc., Mark Zuckerberg and Within Unlimited, Inc.*, Docket No. 9411, 25 August 2022, https://www.ftc.gov/system/files/ftc_gov/pdf/D09411MetaWithinComplaintPublic.pdf

¹⁹⁸ SOMO, *Amazon’s European Chokehold and Monopoly Power* (previously cited).

¹⁹⁹ Yaguara, “21+ Amazon statistics 2025 (Number of Users & Revenue)” (previously cited).

²⁰⁰ SOMO, *Amazon’s European Chokehold and Monopoly Power* (previously cited).

²⁰¹ Amnesty International, *Saudi Arabia: ‘Don’t Worry, It’s a Branch of Amazon’: Exploitation of Migrant Workers Contracted to Amazon in Saudi Arabia* (Index Number: MDE 23/7229/2023), 10 October 2023, <https://www.amnesty.org/en/documents/mde23/7229/2023/en>

²⁰² Amnesty International, *Saudi Arabia: ‘Don’t Worry, It’s a Branch of Amazon’: Exploitation of Migrant Workers Contracted to Amazon in Saudi Arabia* (previously cited).

²⁰³ Amnesty International, *Saudi Arabia: ‘Don’t Worry, It’s a Branch of Amazon’: Exploitation of Migrant Workers Contracted to Amazon in Saudi Arabia* (previously cited).

efficiency over worker welfare.²⁰⁴ Despite being aware of the high risk of labour abuse in Saudi Arabia, Amazon failed to take sufficient action to prevent such abuses or to provide effective and timely remedy when they did.²⁰⁵

Amnesty International wrote to Amazon on 14 June 2023 and 15 August 2023 raising concerns regarding contracted workers in its Saudi Arabia facilities. Amazon responded on 29 July, acknowledging the human rights issues raised and providing an overview of measures taken to fulfil its human rights responsibilities in Saudi Arabia.²⁰⁶ In February 2024, after the release of Amnesty's research, Amazon announced that it had paid \$1.9 million to reimburse more than 700 workers contracted to its operations in Saudi Arabia.²⁰⁷

Amazon has also faced widespread criticism and legal scrutiny for its aggressive stance against unionization efforts across its global operations. The company has been accused of employing a range of union-busting tactics, particularly in the US, where it is alleged that the company surveilled workers,²⁰⁸ held mandatory anti-union meetings,²⁰⁹ and retaliated against organizers.²¹⁰ These practices came under intense public scrutiny during high-profile union drives at US Amazon warehouses in Bessemer, Alabama, and Staten Island, New York. In both cases, the US National Labor Relations Board found that Amazon had violated labour laws, including by interfering with workers' rights to organize.²¹¹

Health and safety concerns at Amazon have also been a long-standing concern raised by trade unions and others. In September 2020, the Reveal programme of The Center for Investigative Reporting published data on injury rates in Amazon warehouses in the US.²¹² The data drew on internal safety reports and weekly injury numbers from Amazon's nationwide network of 150 fulfilment centres between 2016 and 2019. Reveal reported that in 2019: "Amazon fulfilment centres recorded 14,000 serious injuries – those requiring days off or job restrictions. The overall rate of 7.7 serious injuries per 100 employees was 33 per cent higher than in 2016 and nearly double the most recent industry standard."²¹³ Reveal also pointed to a link between the rise in injuries and workload during Prime week (Amazon's annual promotional event) and the holiday peak.²¹⁴

This pattern is not unique to Amazon. Across the tech sector, Big Tech firms have leveraged their economic power to minimize costs and liabilities, often at the expense of workers in the most vulnerable or marginalized situations. Apple has been subject to a number of allegations regarding labour rights abuses in its supply chains.²¹⁵ A 2016 Amnesty International report found that cobalt mined by children and adults in dangerous conditions in the Democratic Republic of Congo was entering the supply chains of major electronics brands, including Apple and Microsoft.²¹⁶ Children as young as seven were found working in hazardous, hand-dug tunnels, exposed to risks like lung damage and physical injury. The cobalt was traced through intermediaries to battery manufacturers supplying Apple, Microsoft and other tech companies.²¹⁷

²⁰⁴ Amnesty International, *Saudi Arabia: 'Don't Worry, It's a Branch of Amazon': Exploitation of Migrant Workers Contracted to Amazon in Saudi Arabia* (previously cited).

²⁰⁵ Amnesty International, *Saudi Arabia: 'Don't worry, It's a Branch of Amazon': Exploitation of Migrant Workers Contracted to Amazon in Saudi Arabia* (previously cited).

²⁰⁶ The full response can be found in Amnesty International, "Saudi Arabia: Amazon response to Amnesty International about contracted workers in its warehouses", 10 October 2023, <https://www.amnesty.org/en/documents/mde23/7237/2023/en>

²⁰⁷ Amazon, "Update on Amazon's response to violations of our supply chain standards involving contracted workers in the Kingdom of Saudi Arabia", 22 February 2024, <https://www.aboutamazon.com/news/company-news/update-on-amazons-response-to-violations-of-our-supply-chain-standards-involving-contracted-workers-in-the-kingdom-of-saudi-arabia>

²⁰⁸ ABC News, "Inside an alleged Amazon union-busting campaign in Kentucky: 'They want to scare us'", 8 December 2023, <https://abcnews.go.com/Business/inside-alleged-amazon-union-busting-campaign-kentucky-scary-story?id=105382727>

²⁰⁹ Reuters, "US labor board bans mandatory anti-union meetings in ruling against Amazon", 13 November 2024, <https://www.reuters.com/technology/us-labor-board-bans-mandatory-anti-union-meetings-ruling-against-amazon-2024-11-13>

²¹⁰ ABC News, "Inside an alleged Amazon union-busting campaign in Kentucky: 'They want to scare us'", (previously cited); Amnesty International, *Amazon, let workers unionize! Respect for workers' rights is not a choice*, 27 November 2020, <https://www.amnesty.org/en/documents/pol40/3275/2020/en>

²¹¹ Reuters, "Amazon must face third union election at Alabama warehouse, NLRB judge rules", 7 November 2024, <https://www.reuters.com/legal/government/amazon-must-face-third-union-election-alabama-warehouse-nlr-judge-rules-2024-11-06>

The Verge, "NLRB judge rules that Amazon broke labor laws in Staten Island (again)", 1 February 2023, <https://www.theverge.com/2023/1/31/23580139/nlr-amazon-labor-union-complaint-solicitation-laws>

²¹² Reveal, "What are injury rates like at Amazon warehouses?", 29 September 2020, <https://revealnews.org/article/amazon-injury-rates>

²¹³ Reveal, "What are injury rates like at Amazon warehouses?" (previously cited).

²¹⁴ Reveal, "What are injury rates like at Amazon warehouses?" (previously cited).

²¹⁵ Business & Human Rights Resource Centre, "Apple accused of violating labour laws as employees at iPhone factory found working 100 hours of overtime, being punished for not meeting targets (incl. co. comments)", 19 September 2021, <https://www.business-humanrights.org/en/latest-news/china-apple-accused-of-violating-labour-laws-as-employees-at-iphone-factory-found-working-100-hours-of-overtime-being-punished-for-not-meeting-targets-incl-co-comments>; Business & Human Rights Resource Centre, "Apple supplier Lens Technology accused of using forced labour in China", 7 January 2021, <https://www.business-humanrights.org/en/latest-news/apple-supplier-lens-technology-accused-of-using-forced-labour-in-china>

²¹⁶ Amnesty International, "Child labour behind smart phone and electric car batteries", 19 January 2016, <https://www.amnesty.org/en/latest/news/2016/01/Child-labour-behind-smart-phone-and-electric-car-batteries>

²¹⁷ Amnesty International, "Child labour behind smart phone and electric car batteries", (previously cited).

Apple's supplier Lens Technology was also accused of using forced labour of Uyghur Muslims in China in 2021.²¹⁸

The market share, connections to a variety of supply chains, and the sheer economic power of Big Tech companies mean they have the ability to significantly shape global labour market conditions. However, companies like Microsoft, Amazon and Apple have also repeatedly failed to assess how their own purchasing practices could contribute to labour rights harms in their supply chains through effective human rights due diligence.²¹⁹ Purchasing practices used by these tech companies such as using "just in time" production, cancelling or changing order volumes and timelines at the last minute due to demand shifts, poor forecasting and low pricing can lead to volatile working conditions for workers of third-party suppliers.²²⁰ Volatility can lead to unpredictable hours – both reduced and increased – which can result in a lack of work or forced overtime and an excessive workload. In a letter to Amnesty International, Microsoft emphasized that the company prohibits forced or child labour and mandates safe, fair working conditions throughout the supply chain through requiring a supplier code of conduct, training, assessments and audits; however, the company declined to comment on the specific cases cited. Amazon and Apple did not respond in writing prior to publication.

Social media companies have also been implicated in serious labour abuses, particularly in outsourced and subcontracted roles. Several cases have been brought against Meta for poor working conditions for content moderators, particularly for those based in Global Majority countries. In March 2023, 184 former content moderators in Kenya brought a case against Meta and Sama – a data labelling company based in Nairobi contracted by Meta for content moderation in Ethiopia – for alleged human rights violations and wrongful termination of contracts.²²¹ The content moderators involved in the litigation complained of constant pressure from managers to work at speed and many also reported suffering from mental health issues such as depression, anxiety, post-traumatic stress disorder and suicidal ideation after spending hours a day reviewing content featuring graphic violence.²²² In August 2023, all parties to the case agreed to mediation, with a view to settling out of court.²²³

Ultimately, rather than fundamentally addressing the issues, Meta simply moved operations to a different partner in a different country – Ghana. In fact, a 2025 investigation by the Bureau of Investigative Journalism and Foxglove Legal revealed that content moderators employed by Meta's new outsourcing partner in Ghana, Teleperformance, faced some of the harshest working conditions documented to date.²²⁴ Moderators reported being subjected to intense psychological strain from reviewing graphic and traumatic content, with inadequate mental health support. The investigation uncovered multiple suicide attempts, arbitrary dismissals, and a culture of fear and silence, with workers allegedly pressured to sign non-disclosure agreements that prevented them from speaking out about their experiences.²²⁵ In a letter to Amnesty International on 25 August 2025, Meta declined to comment on these cases as they relate to active litigation and ongoing regulatory processes.

The abuses of workers' rights documented across Big Tech's operations and supply chains are not isolated incidents – they are systemic outcomes of business models built on cost-cutting, outsourcing and the externalization of risk. Companies like Amazon, Meta, Apple, Microsoft and Google have used their vast market power to shape global labour markets in ways that prioritize flexibility and profit over worker welfare.

²¹⁸ Business & Human Rights Resource Centre, "Apple supplier Lens Technology accused of using forced labour in China" (previously cited).

²¹⁹ Business & Human Rights Resource Centre, *Report: Global ICT Hardware Companies Fail to Address Forced Labor Risks*, 9 January 2023, <https://www.business-humanrights.org/en/from-us/media-centre/report-global-ict-hardware-companies-fail-to-address-forced-labor-risks>

²²⁰ Business & Human Rights Resource Centre, *KnowTheChain ICT Benchmark 2025: Purchasing Practices*, 2 April 2025, <https://www.business-humanrights.org/en/from-us/briefings/knowthechain-ict-benchmark-2025-purchasing-practices>

²²¹ Business & Human Rights Resource Centre, "Content moderators filed a lawsuit against Meta alleging unfair termination of subcontractor's employees and discriminatory hiring conditions", 19 December 2024, <https://www.business-humanrights.org/en/latest-news/kenya-content-moderators-filed-a-lawsuit-against-meta-alleging-poor-working-conditions-including-insufficient-mental-health-support-and-low-pay>

²²² Guardian, "A watershed: Meta ordered to offer mental health care to moderators in Kenya", 7 June 2023, <https://www.theguardian.com/global-development/2023/jun/07/a-watershed-meta-ordered-to-offer-mental-health-care-to-moderators-in-kenya>

²²³ TechCrunch, "Meta and moderators agree to mediation", 23 August 2023, <https://techcrunch.com/2023/08/23/meta-and-moderators-agree-to-mediation/>; In a letter to Amnesty International, Sama said that it disputes the claims made against the company in court and that it is committed to finding a settlement which is agreeable to all parties, and provided details of wellbeing initiatives for content moderators. The full letter is available in Amnesty International, *'A Death Sentence for My Father': Meta's Contribution to Human Rights Abuses in Northern Ethiopia* (previously cited).

²²⁴ The Bureau of Investigative Journalism (TBIJ), "Suicide attempts, sackings and a vow of silence: Meta's new moderators face worst conditions yet", 27 April 2025, <https://www.thebureauinvestigates.com/stories/2025-04-27/suicide-attempts-sackings-and-a-vow-of-silence-metas-new-moderators-face-worst-conditions-yet>

²²⁵ TBIJ, "Suicide attempts, sackings and a vow of silence: Meta's new moderators face worst conditions yet" (previously cited).

From exploitative supply chain practices and union suppression to the psychological toll of outsourced content moderation, these harms are embedded in the architecture of Big Tech's global dominance.

3.7 REGULATORY CAPTURE AND INFLUENCE

The lobbying power of Big Tech is immense. In 2024 in the US alone, Meta reported over \$24 million worth of spending on lobbying,²²⁶ Amazon just under \$18 million,²²⁷ Google over \$12 million,²²⁸ Microsoft over \$9 million²²⁹ and Apple just under \$8 million.²³⁰ In Europe, Google, Meta, Microsoft, Apple and Amazon spent between €35 and €39 million on lobbying in Brussels in 2024 – putting all five companies in the top 10 highest spending corporate lobbyists.²³¹

The level of access these companies command is also significant. According to their own reporting, the five Big Tech companies managed to secure 1,235 high level meetings in Brussels in 2024.²³² For comparison, Amnesty International secured just 96 meetings and this would have covered a number of topics, not just those related to technology.²³³ Around the development of specific legislation, the disparity between corporate and civil society access can be particularly apparent. For instance, in 2023 during the development of the EU's AI Act, it was reported that 86% of meetings on the file with high-level officials at the European Commission were with industry.²³⁴

²²⁶ Meta Platforms, Inc., "Lobbying Report 2024 Q1", published by the United States Senate Lobbying Disclosure Act Reports website, <https://lda.senate.gov/filings/public/filing/44c8cc07-99cb-4a91-83c3-31f973d95281/print> (accessed 1 August 2025); Meta Platforms, Inc., "Lobbying Report 2024 Q2", published by the United States Senate Lobbying Disclosure Act Reports website, <https://lda.senate.gov/filings/public/filing/e3091ff2-c594-4632-af46-a50b47bfb090/print> (accessed 1 August 2025); Meta Platforms, Inc., "Lobbying Report 2024 Q3", published by the United States Senate Lobbying Disclosure Act Reports website, <https://lda.senate.gov/filings/public/filing/8795cb9f-876b-4d1d-a1a6-5ceb8844c2f7/print> (accessed 1 August 2025); Meta Platforms, Inc., "Lobbying Report 2024 Q4", published by the United States Senate Lobbying Disclosure Act Reports website <https://lda.senate.gov/filings/public/filing/8c335706-41da-41f0-9688-dcd4de46bae2/print> (accessed 1 August 2025).

²²⁷ Amazon.com Services LLC, "Lobbying Report 2024 Q1", published by the United States Senate Lobbying Disclosure Act Reports website, <https://lda.senate.gov/filings/public/filing/4329ebb5-a250-407e-8cce-60a9c5ab9fe4/print> (accessed 1 August 2025); Amazon.com Services LLC, "Lobbying Report 2024 Q2", published by the United States Senate Lobbying Disclosure Act Reports website, <https://lda.senate.gov/filings/public/filing/7aa7ca99-9c14-4fc7-ad20-45caa738ca87/print> (accessed 1 August 2025); Amazon.com Services LLC, "Lobbying Report 2024 Q3", published by the United States Senate Lobbying Disclosure Act Reports website, <https://lda.senate.gov/filings/public/filing/f3f53731-47d1-42fa-b09d-e2339702497d/print> (accessed 1 August 2025); Amazon.com Services LLC, "Lobbying Report 2024 Q4", published by the United States Senate Lobbying Disclosure Act Reports website, <https://lda.senate.gov/filings/public/filing/2d06ab44-9b9e-4a24-888b-4bc6b431bfba/print> (accessed 1 August 2025).

²²⁸ Google Client Services LLC, "Lobbying Report 2024 Q1", published by the United States Senate Lobbying Disclosure Act Reports website, <https://lda.senate.gov/filings/public/filing/d715cb88-4878-4ee3-a1dc-b9aed7136aed/print> (accessed 1 August 2025); Google Client Services LLC, "Lobbying Report 2024 Q2", published by the United States Senate Lobbying Disclosure Act Reports website, <https://lda.senate.gov/filings/public/filing/25a4ee4f-fee9-4e5b-9e69-d1e48fa13179/print> (accessed 1 August 2025); Google Client Services LLC, "Lobbying Report 2024 Q3", published by the United States Senate Lobbying Disclosure Act Reports website, <https://lda.senate.gov/filings/public/filing/3e303598-7d0c-47ea-a270-389dc98c062c/print> (accessed 1 August 2025); Google Client Services LLC, "Lobbying Report 2024 Q4", published by the United States Senate Lobbying Disclosure Act Reports website, <https://lda.senate.gov/filings/public/filing/813a7bb1-ae99-4e3b-b2de-89b8952b6cec/print> (accessed 1 August 2025).

²²⁹ Microsoft Corporation, "Lobbying Report 2024 Q1", published by the United States Senate Lobbying Disclosure Act Reports website, <https://lda.senate.gov/filings/public/filing/9160854a-365d-4444-bbbf-df9d91d4bd82/print> (accessed 1 August 2025); Microsoft Corporation, "Lobbying Report 2024 Q2", published by the United States Senate Lobbying Disclosure Act Reports website, <https://lda.senate.gov/filings/public/filing/92c3d49b-737f-4487-a7eb-b617c5afcee7/print> (accessed 1 August 2025); Microsoft Corporation, "Lobbying Report 2024 Q3", published by the United States Senate Lobbying Disclosure Act Reports website, <https://lda.senate.gov/filings/public/filing/f7c48aef-f3c3-46aa-b3da-10df3199efd6/print> (accessed 1 August 2025); Microsoft Corporation, "Lobbying Report 2024 Q4", published by the United States Senate Lobbying Disclosure Act Reports website, <https://lda.senate.gov/filings/public/filing/767443d1-5a99-4c09-a8ca-d092aa1dcbf7/print> (accessed 1 August 2025).

²³⁰ US Apple Association, "Lobbying Report 2024 Q1", published by the United States Senate Lobbying Disclosure Act Reports website, <https://lda.senate.gov/filings/public/filing/23d44ad9-fd1d-4024-a826-f75ab3cd7b14/print> (accessed 1 August 2025); US Apple Association, "Lobbying Report 2024 Q2", published by the United States Senate Lobbying Disclosure Act Reports website, <https://lda.senate.gov/filings/public/filing/4634f9f2-5e1d-4452-b48f-ce6495fc6b9e/print> (accessed 1 August 2025); US Apple Association, "Lobbying Report 2024 Q3", published by the United States Senate Lobbying Disclosure Act Reports website, <https://lda.senate.gov/filings/public/filing/9cb22a32-3a93-4dac-8bb3-afed76408687/print> (accessed 1 August 2025); US Apple Association, "Lobbying Report 2024 Q4", published by the United States Senate Lobbying Disclosure Act Reports website, <https://lda.senate.gov/filings/public/filing/df6bf5b9-e855-4666-aec5-061111fd903e/print> (accessed 1 August 2025).

²³¹ LobbyFacts, "Search | LobbyFacts", <https://www.lobbyfacts.eu/search-all> (accessed 1 August 2025).

²³² LobbyFacts, Meta Platforms Ireland Limited and Its Various Subsidiaries, <https://www.lobbyfacts.eu/datacard/meta-platforms-ireland-limited-and-its-various-subsidiaries-f-k-a-facebook-ireland-limited?rid=28666427835-74> (accessed 1 August 2025); LobbyFacts, Google, <https://www.lobbyfacts.eu/datacard/google?rid=03181945560-59> (accessed 1 August 2025); LobbyFacts, Apple Inc., <https://www.lobbyfacts.eu/datacard/apple-inc?rid=588327811384-96> (accessed 1 August 2025); LobbyFacts, Amazon EU Sarl, <https://www.lobbyfacts.eu/datacard/amazon-eu-sarl?rid=366117914426-10> (accessed 1 August 2025); LobbyFacts, Microsoft Corporation, <https://www.lobbyfacts.eu/datacard/microsoft-corporation?rid=0801162959-21> (accessed 1 August 2025).

²³³ LobbyFacts, Amnesty International European Institutions Office, <https://www.lobbyfacts.eu/datacard/amnesty-international-european-institutions-office?rid=11063928073-34> (accessed 1 August 2025).

²³⁴ Corporate Europe Observatory (CEO), "Big Tech lobbying is derailing the AI Act", 24 November 2023, <https://corporateeurope.org/en/2023/11/big-tech-lobbying-derailing-ai-act>

And this is just direct lobbying. Big Tech companies also have close relationships with think tanks, consulting firms and business/trade associations which also lobby on their behalf and with the priorities of their members. For example, according to the website LobbyFacts – which collates data from the EU Transparency Register, the European Parliament's data on accredited passholders, and the European Commission's data on its high-level lobby meetings – Meta spent between €725,000 and €1.5 million on lobbying work through consulting firms and lawyers in 2024, on top of its own lobbying spending.²³⁵

The business and trade association memberships of many of these corporate lobby groups, and their links to other organizations can be very opaque. In Europe, however, memberships must be declared on the EU Transparency Register. In 2024, Amazon listed 89 memberships and sponsorships on the EU Transparency Register,²³⁶ Meta listed 69,²³⁷ Microsoft 59,²³⁸ Apple 42²³⁹ and Google listed 70.²⁴⁰

All five Big Tech corporations have listed themselves either as direct members or indirect members (through their national member organizations) of The Association of European Employers (BusinessEurope) – the largest lobby group in Brussels – as well as DigitalEurope, the largest digital business association (by lobbying spend). BusinessEurope is a major force in EU policymaking.²⁴¹ Representing organizations from a vast array of sectors, BusinessEurope works on almost all issues of interest to industry, as well as on the development of the European project as a whole. At the forefront of the “Better Regulation” agenda, BusinessEurope has also been a vocal advocate of recent moves by the European Commission to “simplify” – or deregulate – existing EU legislation including legislation related to technology companies such as the General Data Protection Regulation (GDPR) and AI Act.²⁴²

Many Big Tech companies also have close relationships with governments through public sector contracts. Microsoft and Google for example hold public sector contracts across the world.²⁴³ Rather than simply service provision, both of these companies frame these projects as “partnerships” with governments.²⁴⁴ When discussing these partnerships, the Vice President of Global Market Development in Microsoft's Worldwide Public Sector team states “we also recognize that in the context of government operations, the actual technology is just part of the overall conversation; policy and regulatory settings must be considered *and shaped*, so too must the societal objectives of what governments want their country to achieve over the next 30+ years be factored into technology decision making (emphasis added)”²⁴⁵ In other words, Microsoft couples the company's public sector contract provision with influencing regulatory agendas. Given the sheer scale of these contracts globally, the level of access and influence achieved through these contracts is significant.

In the US, Big Tech CEOs have also sought to closely entwine themselves with the Trump administration. The CEOs of Meta, Google, TikTok, Amazon and Apple attended Trump's inauguration. Amazon and Meta contributed \$1 million apiece to Trump's inaugural committee.²⁴⁶ Ahead of the inauguration Meta also announced that it was making a number of changes to its platforms including ceasing fact checking of

²³⁵ This estimate is based on collated figures gathered by LobbyCheck and CEO on the LobbyFacts website and includes spend with the following firms: Trilligent, White & Case LLP, Arthur Cox LLP, EU strategy, Fourtold, NOVE, Oxera Consulting LLP, Vincas Consulting, Utopia Lab S.R.L., Hogan Lovells International LLP; LobbyFacts, <https://www.lobbyfacts.eu> (accessed 1 August 2025).

²³⁶ EU Transparency Register, Amazon EU Sarl, https://transparency-register.europa.eu/searchregister-or-update/organisation-detail_en?id=366117914426-10 (accessed 1 August 2025).

²³⁷ EU Transparency Register, Meta Platforms Ireland Limited and its various subsidiaries, https://transparency-register.europa.eu/search-register-or-update/organisation-detail_en?id=28666427835-74 (accessed on 1 August 2025).

²³⁸ EU Transparency Register, Microsoft Corporation, https://transparency-register.europa.eu/search-register-or-update/organisation-detail_en?id=0801162959-21 (accessed on 1 August 2025).

²³⁹ EU Transparency Register, Apple Inc., https://transparency-register.europa.eu/searchregister-or-update/organisation-detail_en?id=588327811384-96 (accessed on 1 August 2025).

²⁴⁰ EU Transparency Register, Google, https://transparency-register.europa.eu/searchregister-or-update/organisation-detail_en?id=03181945560-59 (accessed on 1 August 2025).

²⁴¹ LobbyFacts, Meta Platforms Ireland Limited and its various subsidiaries (previously cited); LobbyFacts, Google (previously cited); LobbyFacts, Apple Inc. (previously cited); LobbyFacts, Amazon EU Sarl (previously cited); LobbyFacts, Microsoft Corporation (previously cited).

²⁴² BusinessEurope, “Better regulation and burden reduction”, <https://www.buinessurope.eu/policy-priorities/better-regulation-and-burden-reduction> (accessed on 1 August 2025).

²⁴³ For example Microsoft, “New agreement with Microsoft supports government to embrace public cloud”, 29 October 2019, <https://news.microsoft.com/en-xm/2019/10/29/new-agreement-with-microsoft-supports-government-to-embrace-public-cloud>; Microsoft, “Microsoft and G42 announce \$1 billion comprehensive digital ecosystem initiative for Kenya”, 22 May 2024, <https://news.microsoft.com/source/2024/05/22/microsoft-and-g42-announce-1-billion-comprehensive-digital-ecosystem-initiative-for-kenya>; Microsoft, Public Sector, <https://news.microsoft.com/apac/features/public-sector> (accessed 12 August 2024); USAspending.gov, Google LLC, <https://www.usaspending.gov/recipient/eddf926f-f4fe-e72c-14f1-ab22d5925171-C/latest> (accessed 12 August 2025); USAspending.gov, Google Public Sector LLC, <https://www.usaspending.gov/recipient/fa80ed82-5b68-ffce-2167-5a87592ebb7f-C/latest> (accessed 12 August 2025).

²⁴⁴ Google, Google Public Sector, <https://publicsector.google/> (accessed 12 August 2025); Microsoft, “Developing public sector markets together” <https://www.microsoft.com/blog/partnership-approach-pivot> (accessed 12 August 2025).

²⁴⁵ Microsoft, “Developing public sector markets together” (previously cited).

²⁴⁶ Rolling Stone, “Trump's inauguration donors: Big Oil, Big Pharma, Big Tech, Crypto and more”, 31 January 2025, <https://www.rollingstone.com/politics/politics-features/trump-inauguration-donors-big-oil-big-pharma-big-tech-crypto-1235252214>

content.²⁴⁷ Meta's CEO Mark Zuckerberg had also explicitly asked Trump to push back on EU regulatory efforts and fines imposed on Big Tech for anti-competitive practices.²⁴⁸

When lobbying doesn't work, Big Tech companies have been known to abuse their market power by threatening to withdraw from a market. Following a ruling by Nigeria's Federal Competition and Consumer Protection Commission (FCCPC) that found Meta had violated data protection and consumer rights laws, Meta threatened to withdraw its services from the Nigerian market.²⁴⁹ The Director of Corporate Affairs at FCCPC characterized the threat as an attempt to provoke negative public sentiment and pressure the FCCPC to reverse its decision.²⁵⁰

We will likely never fully know the extent of Big Tech's lobbying power as many interactions go unreported and the level of influence of these companies is impossible to quantify. However, we do know that Big Tech are spending a significant amount on lobbying policymakers. We know that these companies often have disproportionate access to decision-makers. And we know that while there have been strides in digital regulation during recent years – such as the Digital Services Act and Digital Markets Act in the EU – legislation that fully addresses the problematic business models of Big Tech is still wanting. Ultimately, lobbying is a tool Big Tech use to ensure they maintain their powerful positions.

²⁴⁷ Meta, Transparency Center, "How fact-checking works", (previously cited).

²⁴⁸ Tech.co, "Zuckerberg asks Trump a favor – Days after Meta moderation revamp", 14 January 2025, <https://tech.co/news/meta-zuckerberg-trump-favor>

²⁴⁹ Rest of World, "What Meta's dispute in Nigeria means for its millions of users", 7 May 2025, <https://restofworld.org/2025/meta-nigeria-fine>

²⁵⁰ Naijanotes, "FCCPC dismisses Meta's market withdrawal threat over consumer protection penalties", 5 May 2025, <https://naijanotes.net/fccpc-dismisses-metas-market-withdrawal-threat-over-consumer-protection-penalties>

4. THE NEXT PHASE: DOMINANCE IN GENERATIVE ARTIFICIAL INTELLIGENCE

The next phase of Big Tech's consolidation of power is unfolding through the rapid expansion of generative artificial intelligence (AI). In recent years this boom has captured the world's attention. While the emergence of generative AI might have initially suggested an opportunity for new entrants to challenge Big Tech, the reality is that the same dominant actors – Microsoft, Google, Meta and Amazon – are exerting their control over this growing market and further embedding business models which are predicated on the abuse of human rights.

As well as developing their own generative AI models such as Google's Gemini and Meta's LLaMA, Big Tech are deeply entwined with emerging AI companies such as OpenAI – backed by Microsoft – and Anthropic, backed by Google and Amazon.²⁵¹ Despite their sky-high valuations, these smaller firms operate at significant losses, with no clear path to profitability – making them dependent on continued investment from the very corporations they might otherwise compete with.

The primary type of generative AI being developed, and invested in, by Big Tech is based on Large Language Models (LLMs). LLMs are machine learning models trained on vast amounts of text data to process and generate human-like language. Similarly to the business models of some Big Tech companies (see for example section 3.1 “Excessive data collection and the right to privacy”), the data practices underpinning these models raise serious privacy concerns. Generative AI models are trained on vast datasets scraped from the web, often without proper consent. Reports indicate that ChatGPT for example used a web scraper to gather training data – including at least 60 million domains over the course of 12 years.²⁵² Google's 2023 Privacy Policy update confirmed that its web crawling infrastructure – currently deployed for its search function – is now being used to train AI models.²⁵³ The sheer size of the data collection already being undertaken by Google and Meta has put them in a strong position to also dominate in this new market. Meta's CEO, Mark Zuckerberg, has openly stated that the company's competitive edge in generative AI lies in its access to hundreds of billions of publicly shared images and tens of billions of public videos.²⁵⁴ Meanwhile, in January 2024, OpenAI was accused by Italy's data protection authority of violating the GDPR

²⁵¹ AI Now Institute, *Artificial Power: AI Now 2025 Landscape*, 3 June 2025, <https://ainowinstitute.org/publications/research/ai-now-2025-landscape-report>

²⁵² TechCrunch, “Here are a few ways GPT-3 can go wrong”, 7 August 2020, <https://techcrunch.com/2020/08/07/here-are-a-few-ways-gpt-3-can-go-wrong>

²⁵³ Google, Privacy Policy (previously cited).

²⁵⁴ MassMark Media, “Meta's bold vision: How Zuckerberg plans to surpass Google and Microsoft in the AI race”, 6 January 2025, <https://massmarkmedia.com/meta-ai-strategy-google-microsoft-competition>

through its data scraping practices. OpenAI claims its actions are justified under a public interest exception under GDPR.²⁵⁵

In their letters to Amnesty International Microsoft and Meta both emphasized their commitments to user privacy. However, Amnesty International's concerns around AI and privacy remain. While some companies offer opt-out mechanisms for users who do not want their data used in AI training, these are not always effective.²⁵⁶ The "opt-outs" often do not apply retroactively to data already scraped, and there are challenges applying them to third-parties.²⁵⁷ In 2024, noyb (none of your business) – a European privacy rights organization – filed 11 complaints against Meta across Europe, alleging that Meta's plan to use years of personal posts, images and tracking data for undefined AI purposes violated the GDPR.²⁵⁸ Following these complaints Meta agreed to pause its plans to train AI models using public content from Facebook and Instagram users in the EU and European Economic Area.²⁵⁹

Big Tech companies are rapidly building and deploying AI systems, prioritizing speed and scale over fairness and accuracy. We know that AI models trained on flawed or biased datasets produce outcomes that disadvantage individuals based on race, socio-economic status, gender, disability, sexual orientation or age. Those who are already marginalized – such as migrants, asylum seekers, job applicants, or individuals relying on public services – are particularly vulnerable to harms stemming from algorithmic profiling and biometric mass surveillance. Amnesty International research in Denmark for example showed how AI tools used by the Danish government to detect benefit fraud risks discriminated against people with disabilities, low-income individuals, migrants, refugees and racialized groups.²⁶⁰ The AI systems currently being prioritized by Big Tech based on data scraped from the internet, risk perpetuating and amplifying existing forms of social bias, discrimination, and inequality.

Big Tech dominance in the generative AI market also risks replicating the types of labour rights abuses already present in the operations and supply chains of these companies. Much of the labour that powers generative AI – particularly data annotation – is outsourced to low-income countries where workers do much of the gruelling work involved in preparing structured datasets for deep learning in generative AI algorithms.²⁶¹ In late 2024 and early 2025, lawsuits were filed against Scale AI alleging poor working conditions, exploitive behaviour, widespread wage theft, predatory labour practices, and the repeated exposure of workers to unsafe and emotionally distressing content, leading to cases of post-traumatic stress disorder.²⁶²

While generative AI applications dominate headlines, much of the profit lies in the cloud infrastructure that powers them. Generative AI systems require immense computational power, which in turn depends on vast cloud infrastructure. Microsoft, Amazon, and Google collectively control over 60% of the global cloud market.²⁶³ These companies are not just AI developers – they are landlords of the digital infrastructure on which all generative AI, and therefore AI developers – depend. This positions them to extract value from the entire ecosystem, regardless of which AI applications succeed or fail.²⁶⁴ However, the data centres – groups of high performing servers – needed to support generative AI consume enormous amounts of energy and water, directly impacting the environment.²⁶⁵ Google's own sustainability report from 2024 noted a staggering 48% increase in greenhouse gas emissions since 2019, attributable to data centre and supply chain

²⁵⁵ TechCrunch, "ChatGPT is violating Europe's privacy laws, Italian DPA tells OpenAI", 29 January 2024, <https://techcrunch.com/2024/01/29/chatgpt-italy-gdpr-notification>

²⁵⁶ TechCrunch, "Bluesky's open API means anyone can scrape your data for AI training", 27 November 2024, <https://techcrunch.com/2024/11/27/blueskys-open-api-means-anyone-can-scrape-your-data-for-ai-training>

²⁵⁷ TechCrunch, "Bluesky's open API means anyone can scrape your data for AI training" (previously cited).

²⁵⁸ NOYB, "noyb urges 11 DPAs to immediately stop Meta's abuse of personal data for AI", 6 June 2024, <https://noyb.eu/en/noyb-urges-11-dpas-immediately-stop-metas-abuse-personal-data-ai>

²⁵⁹ NOYB, "(Preliminary) noyb WIN: Meta stops AI plans in the EU", 14 June 2024, <https://noyb.eu/en/preliminary-noyb-win-meta-stops-ai-plans-eu>

²⁶⁰ Amnesty International, *Coded Injustice: Surveillance and Discrimination in Denmark's Automated Welfare State* (Index Number: EUR 18/8709/2024), 12 November 2024, <https://www.amnesty.org/en/documents/eur18/8709/2024/en>

²⁶¹ TIME, "OpenAI used Kenyan workers on less than \$2 per hour to make ChatGPT less toxic", 18 January 2023, <https://time.com/6247678/openai-chatgpt-kenya-workers>; TIME, "New global safety standards aim to protect AI's most traumatized workers", 19 June 2025, <https://time.com/7295662/ai-workers-safety-rules>

²⁶² Computerworld, "Scale AI sued by former worker alleging unlawful business practices", 12 December 2024, <https://www.computerworld.com/article/3624021/scale-ai-under-fire-in-suit-filed-by-former-worker-alleging-unlawful-business-practices.html>; TechCrunch, "Scale AI hit by its second employee wage lawsuit in less than a month", 9 January 2025, <https://techcrunch.com/2025/01/09/scale-ai-hit-by-its-second-employee-wage-lawsuit-in-less-than-a-month>; TechCrunch, "Scale AI is facing a third worker lawsuit in about a month", 22 January 2025, <https://techcrunch.com/2025/01/22/scale-ai-is-facing-a-third-worker-lawsuit-in-about-a-month>

²⁶³ Statista, "Amazon and Microsoft stay ahead in global cloud market", 27 February

2025, <https://www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers>

²⁶⁴ AI Now Institute, *Artificial Power: AI Now 2025 Landscape* (previously cited).

²⁶⁵ IEEE Technology Climate Center, "The hidden cost of AI: Unpacking its energy and water footprint", 25 February 2025, <https://itcc.ieee.org/blog/the-hidden-cost-of-ai-unpacking-its-energy-and-water-footprint>

emissions.²⁶⁶ These environmental costs are largely hidden from public view, yet they are central to the generative AI boom.

Regulators are beginning to respond to the growing concentration of power in the generative AI ecosystem. In 2024 in the US, the FTC and the DOJ launched an antitrust investigation into Microsoft, OpenAI and Nvidia, focusing on whether their partnerships and market behaviour were stifling competition in the AI sector.²⁶⁷ Microsoft's \$13 billion investment in OpenAI, in particular, has drawn scrutiny for potentially giving it significant influence over a key player in the generative AI market.

In the EU, Microsoft's partnership with OpenAI avoided a formal merger probe, but regulators are still examining the exclusivity clauses in their agreements, which may limit competition by locking OpenAI into Microsoft's Azure cloud infrastructure.²⁶⁸ Meanwhile, reports in June 2025 revealed that OpenAI executives allegedly discussed accusing Microsoft of anti-competitive behaviour, suggesting growing internal tensions over control and independence.²⁶⁹

On 12 August 2025, Amnesty International wrote to Microsoft, Meta, Google and Amazon raising concerns around potential negative human rights impacts related to the generative AI sector. Google and Amazon did not respond in writing before publication, and Meta did not explicitly address the generative AI-related allegations addressed to them. Microsoft highlighted that they are guided by AI Principles when building and deploying AI, that the company is committed to environmental sustainability and underscored their AI empowerment initiatives.²⁷⁰ However, the human rights impacts of Big Tech's consolidation of market power in this new and evolving sector was not explicitly addressed.

In short, the generative AI boom is not a story of innovation, progress and new tech powers, but a story of consolidation, extraction and control. It represents a new phase in the expansion of Big Tech's power – one that threatens to further embed systems that harm our rights. Without urgent regulatory intervention, the dominance of these firms in generative AI will take us ever further from an online world built on the rights of users.

²⁶⁶ Google, *Google 2024 Environmental Report*, July 2024, <https://www.gstatic.com/gumdrop/sustainability/google-2024-environmental-report.pdf>

²⁶⁷ CNBC, "U.S. regulators to open antitrust probes into Nvidia, Microsoft and OpenAI", 6 June 2024, <https://www.cnbc.com/2024/06/06/us-regulators-to-open-antitrust-probes-into-nvidia-microsoft-and-openai.html>

²⁶⁸ Global Competition Review, "AI partnerships: Microsoft/OpenAI avoids EU merger probe, exclusivity clauses draw scrutiny", 28 June 2024, <https://globalcompetitionreview.com/article/ai-partnerships-microsoftopenai-avoids-eu-merger-probe-exclusivity-clauses-draw-scrutiny>

²⁶⁹ Reuters, "OpenAI executives have discussed accusing Microsoft of anticompetitive behavior: WSJ", 17 June 2025, <https://www.businesstimes.com.sg/companies-markets/telcos-media-tech/openai-executives-have-discussed-accusing-microsoft-anticompetitive-behavior-wsj>

²⁷⁰ Microsoft, "Microsoft responsible AI: Principles and approach", <https://www.microsoft.com/en-us/ai/principles-and-approach?msocid=15b26cb126ee63e425ed7fee27ad6261> (accessed 26 August 2025)

5. THE ROLE OF COMPETITION LAW IN STATES' HUMAN RIGHTS OBLIGATIONS

Under international law, states have an obligation to respect, protect and fulfil human rights. The UN Guiding Principles on Business and Human Rights (UN Guiding Principles) explicitly outline that such a duty applies in the context of corporate activities.²⁷¹ The legal obligation to protect individuals from human rights abuses by corporations requires states to prevent harm through regulation, investigate abuses, hold perpetrators accountable and ensure access to effective remedies.

The UN Guiding Principles do not prescribe a single approach for how states should meet these obligations. Instead, they encourage States to adopt a “smart mix” of measures – national and international, mandatory and voluntary – to foster business respect for human rights.²⁷² This includes enforcing existing legislation which directly or indirectly regulates business respect for human rights. The UN Guiding Principles acknowledge that the implications for human rights of legislation outside of the human rights field such as corporate law remain poorly understood. Yet these legal frameworks directly shape business behaviour and have the ability to reinforce or undermine human rights protections.²⁷³ Furthermore, as UN Guiding Principle 3 notes, “the failure to enforce existing laws that directly or indirectly regulate business respect for human rights is often a significant legal gap in State practice.”²⁷⁴

The human rights harms linked to market dominance are evident. As outlined in this briefing, digital platforms with unchecked market power can shape public discourse, impose unfair terms and conditions, perpetrate harmful labour abuses and collect vast amounts of personal data undermining the right to privacy. The abuse of dominance has also entrenched the surveillance-based business model as the default model across social media, search, operating systems and more, crowding out the potential for rights-respecting alternatives.

Thus, it is consistent with international law frameworks that states must act to address the human rights harms linked to the abuse of dominance of several Big Tech companies. While new regulation may be necessary, existing competition and antitrust frameworks already provide powerful tools – including investigative powers and binding structural and behavioural remedies – that can be used to in part fulfil the state duty to protect human rights.

²⁷¹ UN, *Guiding Principles on Business and Human Rights: Implementing the UN ‘Protect, Respect and Remedy’ Framework (UNGPs)*, 2011, UN Doc HR/PUB/11/04, Principle 1.

²⁷² UN, *UNGPs* (previously cited), Principle 3.

²⁷³ “Laws and policies that govern the creation and ongoing operation of business enterprises, such as corporate and securities laws, directly shape business behaviour. Yet their implications for human rights remain poorly understood.” UN, *UNGPs* (previously cited).

²⁷⁴ UN, *UNGPs* (previously cited), Principle 3.

However, any such use of competition law and antitrust frameworks to advance human rights objectives must be approached with care. It is crucial that states – and competition authorities working on behalf of the state – tread carefully when utilizing competition law for human rights aims. For example, structural remedies such as breaking up dominant companies is a key measure that regulators can implement when companies are found to be abusing their dominant position. However, breaking up Big Tech companies such as Facebook and Google may not fully address their harms and could lead to unintended consequences if not done carefully. Smaller companies operating similar problematic business models may still pose serious risks to rights, even if their data collection and reach is more limited.

To be effective, states should empower competition authorities to adopt a mix of structural and behavioural remedies when companies are found to be negatively impacting on human rights through abuse of their dominant position. Structural measures may include break-ups, divestitures, asset transfers, or blocking future mergers and acquisitions. Behavioural measures such as mandatory interoperability (e.g. requiring social media platforms to interact like email services) and data portability can allow users to leave a service and remain connected.

Similarly, states developing or implementing more traditional corporate accountability approaches such as the development of mandatory human rights due diligence legislation for companies must ensure that companies are required to consider the human rights risks and harms that could be linked to market dominance. The UN Guiding Principles stipulate that to meet the corporate responsibility to respect human rights, 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. The UN Guiding Principles also acknowledge that human rights situations are dynamic and therefore “assessments of human rights impacts should be undertaken at regular intervals: prior to a new activity or relationship; prior to major decisions or changes in the operation (e.g. market entry, product launch, policy change, or wider changes to the business)”. Given the potential human rights impacts of market dominance, a company should therefore be expected to conduct a human rights risk assessment as part of its ongoing human rights due diligence before, during and after a merger or acquisition to determine the impact of this shift on human rights.

Competition authorities should also work closely with other state authorities such as data protection authorities and human rights bodies to ensure they have a holistic understanding of the human rights implications of competition decisions. For instance, when the FCCPC imposed on Meta a \$220 million penalty fine and remedies for abuse of market power and privacy violations the authority enforced three laws simultaneously: consumer protection, data protection and competition law, with the investigation conducted jointly with the Nigeria Data Protection Commission (NDPC). This collaboration led to a nuanced judgement which acknowledged that: “Data protection has been vastly recognised as a consumer protection issue, but very few have recognised the increasing concern and challenges it raises as a competition issue.”²⁷⁵

Competition law and antitrust are not a silver bullet for the enforcement of international human rights obligations, but they are a critical and underutilized tool in the state’s human rights toolbox. When applied thoughtfully, these existing laws can help dismantle harmful concentrations of power and create space for a more pluralistic, rights-respecting digital ecosystem and thus should be considered an important instrument through which states could implement their human rights obligations.

²⁷⁵ Federal Competition and Consumer Protection Commission, “Executive summary: Investigation into WhatsApp’s updated privacy policy and consumer rights violations”, 13 November 2023, https://fccpc.gov.ng/wp-content/uploads/2024/07/Excutive_Summary-_WhatsApp_Investigation-13.11.23.pdf

6. CONCLUSION AND RECOMMENDATIONS

The significant market power of Big Tech – Meta, Google, Microsoft, Amazon, and Apple – has accumulated over the last few decades, sometimes through anti-competitive strategies, such that these five companies now control many of the services we use to access the internet as well as the associated infrastructure such as smartphone operating systems.

This dominant position has allowed these companies to normalize business models which in many cases are incompatible with our rights. Meta and Google have created a world in which ubiquitous surveillance of users and reckless, profit-oriented algorithmic curation of content has become a normal feature of the internet, despite the pervasive negative human rights impacts they entail. And yet none of these features are necessary to enable the enjoyment of our human rights online. Human rights-respecting alternatives are possible.

States have an obligation under international human rights law to respect, protect and fulfil human rights including by regulating and using other measures to keep corporate power in check. Competition and anti-trust law provides one such tool which regulators can and should use to ensure the dominant position of these companies does not further harm human rights including implementing the following recommendations.

- Investigate Amazon, Microsoft, Google, Meta, Apple and, where relevant, other powerful technology companies for potential human rights harms linked to their market power and anticompetitive practices.
- Where human rights harm linked to market power and anticompetitive practices are identified, States should:
 - Pursue behavioural and structural remedies, including the break-up of dominant companies.
 - Ensure proposed remedies are fully rights-respecting including by conducting a human rights impact assessment to assess how the remedies will impact human rights and by working closely with human rights bodies to draw on their human rights expertise.²⁷⁶
 - Prevent re-consolidation through stringent merger controls.
- Investigate the emerging generative AI sector – including AI foundation model developers and infrastructure providers (e.g. data, cloud, chips) – to establish human rights risks and impacts linked to anticompetitive practices and market power including conducting ex ante reviews of Big Tech partnerships with AI companies.
- Where human rights harm linked to market power and anticompetitive practices in the generative AI sector are identified:

²⁷⁶ For example, breaking up companies which operate a surveillance-based business model into smaller companies operating similar models does not fully address the human rights issue. Therefore, a package of remedies alongside break ups must be considered to ensure that the human rights impact is fully addressed. This is why it is essential that competition authorities conduct human rights impact assessment to assess the impacts of proposed remedies on human rights, as well as work closely with human rights authorities. This will also help to mitigate the risk of unintended negative impacts on human rights.

- Pursue behavioural and structural remedies, including requiring Big Tech to divest from AI companies as well as breaking up dominant companies where appropriate.
- Enact and enforce stringent merger controls to prevent re-consolidation and companies gaining simultaneous access to different areas of the generative AI markets (e.g. cloud, chip designers and AI development companies).
- Enact rules against self-preferencing by cloud providers and AI development companies, that is, prevent companies from favouring their own services over third-party services.
- Ensure proposed remedies are fully rights-respecting, including by conducting a human rights impact assessment to assess how the remedies will impact human rights, and working closely with human rights bodies to draw on their human rights expertise.
- Require cooperation between different authorities such as competition authorities, data protection regulators, human rights bodies, and consumer bodies to share evidence and expertise, conduct joint investigations and ensure enforcement that addresses the full range of harms.
- Require competition authorities to integrate human rights risk assessments and considerations into competition enforcement, including details on how market dominance and/or mergers may affect rights during competition investigations and merger reviews to ensure that potential human rights impacts are assessed and addressed during competition decisions.
- Legally require companies, including technology companies, to conduct human rights due diligence on their business operations, products and services, as well as their business relationships and report publicly on their due diligence policies and practices in accordance with international standards. This legislation should require human rights due diligence which:
 - Includes risks related to market power and data consolidation.
 - Mandates that companies conduct human rights impact assessments before, during and after mergers or acquisitions.
- Block mergers and acquisitions that significantly risk harming human rights.
- Require that digital platforms:
 - Support systems interoperability, meaning their products and services can work seamlessly with those of other providers (e.g. messaging across platforms), so that users have more choice.
 - Support data portability so users can switch services without losing their networks or content.
- Where they do not exist, introduce rules to prevent outsized lobbying power, including:
 - Conflict-of-interest rules for public officials moving from lobbying roles at Technology companies.
 - Transparency of lobbying activities and funding of think tanks or trade associations by corporations.

ANNEX

Microsoft Corporation

www.microsoft.com



August 25, 2025

Re: Microsoft's Commitment to Human Rights – Response to Amnesty International Inquiry

Dear [REDACTED]

Thank you for the opportunity to share information relevant to Amnesty International's forthcoming report.

Microsoft is firmly committed to respecting human rights across our business and value chain, as set forth in our [Global Human Rights Statement](#). This commitment is inseparable from our mission to empower every person and organization on the planet to achieve more: we believe that people will only use technologies they trust, and they will only trust technologies that respect their rights and advance human dignity.

Guided by international standards like the UN Guiding Principles on Business and Human Rights, we have integrated human rights due diligence, including identification, prevention, and mitigation of adverse impacts, into our governance and everyday operations. We prioritize transparency and accountability, publicly reporting on our progress and making grievance and effective remedy mechanisms available.

In response to your inquiry, we wanted to highlight just a few of our efforts to respect human rights throughout our business.

Supply chain responsibility and sustainability. We hold ourselves and our suppliers to strict standards to uphold human rights and environmental responsibility. Microsoft's Global Human Rights Statement and [Supply Chain Human Rights Policy Statement](#) expressly **prohibit forced or child labor and mandate safe, fair working conditions** throughout our supply chain. We require suppliers to comply with our [Supplier Code of Conduct](#), and we reinforce these expectations through training, assessment, and audits. Our supply chain human rights program extends to raw materials as well. As demonstrated by our

Microsoft Corporation is an equal opportunity employer.



[Responsible Sourcing of Raw Materials Policy](#), we require that upstream suppliers implement ethical practices in accordance with the OECD due diligence guidance, and we collaborate with initiatives like the Responsible Minerals Initiative and the Initiative for Responsible Mining Assurance to drive improvements on the ground.

We are equally committed to **environmental sustainability**. Microsoft has set [ambitious environmental goals](#), including a goal to become carbon negative and water positive in the coming years. We are investing in innovations to reduce our carbon footprint and in community projects that replenish water and protect ecosystems, reflecting our belief that a healthy planet is essential for the enjoyment of fundamental rights.

Responsible technology, AI skilling, and privacy. As we develop new technologies, we prioritize ethical and inclusive design to ensure they uphold human rights. Microsoft was one of the first companies to establish comprehensive [AI Principles](#)—fairness, reliability & safety, privacy & security, inclusiveness, transparency, and accountability—to guide how we build and deploy AI. We've operationalized these principles through a company-wide [Responsible AI Standard](#) with oversight from Office of Responsible AI. We also continuously refine our practices and share learnings openly (for example, by publishing an annual [Responsible AI Transparency Report](#)) to help advance responsible AI governance across our industry.

In parallel, we are investing in **AI skilling and empowerment** initiatives to ensure the benefits of technology are broadly shared. Since 2020, Microsoft and LinkedIn have helped train and certify [more than 14 million people](#) worldwide in digital and AI skills—including members of underserved communities—through free coursework, certifications, and partnerships with over 400 nonprofit organizations. By equipping individuals with these future-ready skills, we aim to foster inclusive economic opportunity and help workers thrive alongside advancing AI.

We are also committed to **expanding connectivity** in underserved communities around the world—recognizing that digital inclusion is foundational to ensuring no one is left behind in the AI era. In partnership with others, we have helped bring internet access to more than 100 million people globally, with a goal of reaching

Microsoft Corporation is an equal opportunity employer.



250 million by the end of 2025, including 100 million in Africa. Importantly, this access is not conditioned on the use of Microsoft products or services—we view connectivity as a fundamental enabler of opportunity in the digital age and a critical first step in extending the benefits of technology and AI to everyone.

Furthermore, **privacy** and data security remain central to our approach. We are deeply committed to protecting users' privacy rights, giving people robust controls over their personal data and advocating for strong global privacy laws. We build our products and cloud services with strict privacy safeguards and transparency, so customers and individuals can trust that their information is handled responsibly and in line with our privacy commitments.

Open innovation. Finally, it is worth noting that Microsoft Windows and Azure are both **open platforms** that enable customers to use them as interoperable tools. Many independent software vendors have successful businesses on our platforms empowering them to achieve their unique goals.

For example, **Windows** allows applications to be installed from any source, without the need to get Microsoft's permission or any fee from Microsoft. As your letter mentioned browsers from the early 2000s, we would highlight that Windows is open to any browser maker, and Windows users can and do choose to use many other browsers besides Microsoft's own browser Microsoft Edge. Microsoft Edge's share of [global browser usage](#) on desktop devices is less than 12 percent, meaning well over 80 percent of all browser time on a desktop/laptop device is done in a non-Microsoft browser.

Azure is similarly open, supporting customers' desire to use [multiple clouds](#) as well as thousands of available third-party apps and services. As is the case with Windows, customers decide what apps and services they want to use and pick and choose what best serves their needs.

To meet customer demand, Microsoft offers a full suite of **productivity services** that includes communication and collaboration functionality, including Teams, Outlook, Office, etc. Indeed, modern productivity cannot be accomplished without offering the ability for multiple users, including those working on different platforms, to collaborate.

Microsoft Corporation is an equal opportunity employer.

Microsoft Corporation

www.microsoft.com



With all of these products and services, customers ultimately determine what solutions work best for them, and Microsoft offers industry-leading interoperability to ensure customers who choose different solutions are able to continue to work with Microsoft products.

Looking ahead, Microsoft remains steadfast in our human rights commitment. We view this work as an ongoing journey of improvement. We will continue to engage with stakeholders—including civil society organizations like Amnesty International, multistakeholder groups (such as Global Network Initiative and Responsible Business Alliance), community groups, and directly impacted rightsholders—to inform our efforts and to collaborate on solutions that enhance respect for human rights across the technology sector.

We appreciate the role that your organization and others play in holding companies accountable. Please know that we share the common goal of a world where technology supports and elevates human rights. We are committed to working every day to earn trust and use our innovation to benefit people and communities globally.

Thank you again for reaching out.



Corporate Vice President, Trusted Technology Group

Microsoft Corporation

Microsoft Corporation is an equal opportunity employer.



August 25, 2025

Amnesty International
Peter Benenson House
1 Easton Street
London, WC1X 0DW
United Kingdom

Attention: [REDACTED]

August 25, 2025

Dear [REDACTED]

We acknowledge receipt of your letter dated August 12, 2025, regarding Amnesty International's forthcoming report. We're grateful for and respect Amnesty's continued commitment to advancing human rights.

We are also writing to highlight that the draft material you shared makes multiple inaccurate claims on a broad range of topics, including those related to active litigation and ongoing regulatory processes. As you may already be aware, that limits our ability to discuss those topics in detail.

We've also responded previously, in detail, to many of the prior Amnesty reports you cite as reference material. (For example, we are re-attaching our letter on Ethiopia of 25 October 2023).

As a result, it's probably most useful to direct you and your members to our existing detailed and relevant disclosure reports:

- We believe it's important to communicate with rights holders about our human rights work in an open and transparent way. In addition to our significant [regulatory and transparency reporting](#), Meta also discloses detailed information on our human rights risk management processes, including crisis and conflict response, in [our annual human rights report](#) (available in multiple languages). This is in line with our [corporate human rights policy](#). We prioritize and report our most salient human rights risks in line with

our comprehensive salient risk assessment, disclosed in detail in our [2022 human rights report](#).

- Our annual human rights report complements our [Responsible Business Practices Report](#), which offers a detailed look at our progress in addressing social and environmental priorities, as well as our efforts to create sustainable value for our customers, employees, investors and other stakeholders. It focuses on the key topics identified throughout our stakeholder engagement process, including public policy and engagement strategies, well-being, competition, and privacy policies.

Every day, people choose to use Facebook, Instagram, Messenger and Threads to share their experiences, discover, create and share content and topics that are of interest to them, connect with friends and family, and build communities. Our apps and services operate in a highly competitive landscape such that we constantly need to innovate in order to improve our offerings and give people opportunities to create and freely express themselves across countries and cultures and in dozens of languages.

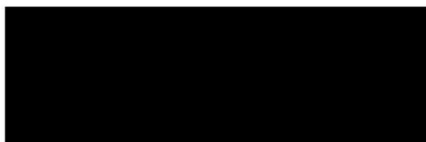
Meta recognizes how important it is for our platforms to be places where people feel empowered to communicate, and we take our role seriously in keeping abuse off our services. That's why we take action on content, like hate speech, bullying, or harassment, that violates our [Community Standards](#), and provide people tools like reporting and blocking to let us know if there may be a violation and avoid further interactions. It's also why we continue to invest in new technologies and methods to help protect people on our platforms. More information and transparency reporting is available at our [Transparency Center](#).

Additionally, we provide ways for users to control their online experiences and the kind of content they see. On Instagram, [for example](#), you can choose who you see in your feed and change your feed to be in chronological order. We also provide controls like the Not Interested tool, the ability to hide posts containing specific words in the caption or hashtag, and Sensitive Content Control, which allows people to see more or less of some types of sensitive content and accounts on Instagram. We have also published [22 system cards](#) that contain information and actionable insights everyone can use to understand and customize their specific AI-powered experiences in our products.

Privacy is at the core of everything we build. We've made extensive progress in overhauling our privacy practices and invested more than \$8 billion in our privacy program since 2019. We've applied the lessons we learned in building the privacy program to all product compliance efforts across Meta. At the heart of this investment are the teams, technology and processes that build privacy protections into our products and create the oversight and accountability for a mature privacy program at an unprecedented scale. We've strengthened our [privacy policies](#) and built new tools to give people even more control of their experiences. From end-to-end encryption on Messenger to Instagram Teen Accounts and privacy tools in Quest headsets, we're dedicated to creating safer, more secure experiences for the nearly four billion people who use our products every day. For more information see: [Privacy Progress](#).

We will continue this work, and welcome robust dialogue with Amnesty International and other civil society organizations as we continue to address the complex challenges you outline.

Yours sincerely,



Director, Human Rights Policy

Encl: Meta letter of October 25, 2023 to Amnesty International



October 25, 2023

[REDACTED]
Programme Director
Amnesty Tech
Amnesty International
1 Easton Street,
London, WC1X 0DW,
United Kingdom
by email

Dear [REDACTED]

Thank you for reaching out regarding Amnesty International's intention to publish the draft report mentioned in your 11 October 2023 letter (Amnesty reference: TC AFR 25/2023.4613).

In these circumstances, I regret I'm unfortunately not in a position to comment further.

The content of the draft report pertains to matters currently subject to litigation involving Meta Platforms, Inc. ("Meta") before the High Court of Kenya (Petition No. E541 / 2022), in which Amnesty International is involved as an Interested Party. As such, given rules against parties to a dispute publicizing matters that are under consideration by Kenyan courts, Meta respectfully declines to provide detailed comments on the allegations outside the ongoing proceedings and reserves its rights.

We fundamentally disagree with the conclusions Amnesty International has reached in the draft report as they are in fact unproven *allegations* made by Petitioners in the above referenced litigation.

The allegations of wrongdoing against Meta in the draft report ignore important context and facts including, for example,

- (i) that Ethiopia has been one of our highest priorities for country-specific interventions, and
- (ii) Meta's significant and ongoing efforts to curb violating content on Facebook related to Ethiopia.

Details of these are available in our Letter to Amnesty International of 18 September 2023, as well as in our 2021 [annual Human Rights Report](https://humanrights.fb.com/wp-content/uploads/2023/09/2021-Meta-Human-Rights-Report.pdf), available online at <https://humanrights.fb.com/wp-content/uploads/2023/09/2021-Meta-Human-Rights-Report.pdf>.

Yours sincerely,



Director, Human Rights Policy

Attached: Letter to Amnesty International of 18 September 2023



September 18, 2023

[REDACTED]
Programme Director
Amnesty Tech
Amnesty International
1 Easton Street,
London, WC1X 0DW,
United Kingdom
by email

Dear [REDACTED]

Thank you for your letter of July 18.

First, we believe it may be useful to begin by including information we published May 2022 in response to the Oversight Board, publicly available at [Meta Q1 2022 Quarterly Update on the Oversight Board](#):

The global Human Rights team has worked as an integral part of the At Risk Countries (ARC) program since 2019. An overview of our approach to countries at risk can be found in [our Transparency Center](#). The team has embedded standards and principles from the UN Guiding Principles on Business and Human Rights (UNGPs) into relevant prioritization and analytical frameworks, which serve as ongoing due diligence tools. Shortly after our global Human Rights team was created, Ethiopia's risk level was re-evaluated, a third party fact checking assessment program was established, and other colleagues were trained on atrocity crime risks and frameworks. Human Rights staff have also participated in Ethiopia risk management processes on an ongoing basis since 2019.

Since early 2020, due diligence has included field-based information gathering and research, focused stakeholder engagement, and formal due diligence from

the Business and Human Rights Group in partnership with our Africa Public Policy team. An updated Human Rights Impact Assessment (HRIA) focused on risk mitigation ahead of Ethiopia's elections was finalized in June 2021.

In 2022, members of the cross-functional team of Meta staff visited Addis Ababa for three days to meet with a wide array of stakeholders that included: the Prime Minister's Office, various government agencies, human rights activists, CSOs, our Trusted Partners, and independent institutions including the Ethiopia Media Authority and the Ethiopia Human Rights Commission. The team has also engaged with new stakeholders about our Community Standards, digital security, safety and privacy standards, connectivity work, and our socio-economic impact initiatives.

This extensive and multi-layered due diligence and stakeholder engagement has informed our approach to content moderation and product development for the region. Our human rights teams continue to support Content Policy teams to understand the humanitarian situation, codewords, and slurs being used on the ground. Relevant members of our Content Policy teams have also received law of armed conflict training. We can now review content in the top four languages spoken and those central to the conflict (Amharic, Oromo, Somali, Tigrinya). Additionally, we have created solutions that make it easier for Ethiopians, as well as specialized international and local human rights and civil society organizations, to notify us when they see potentially violating content, so we can investigate it for possible violations. As stated previously in response to the Board's recommendation, we will continue to conduct thorough human rights due diligence and dynamic risk management processes in Ethiopia, and share insights and actions from our due diligence that aligns with the board's recommendations, our Human Rights Policy, and the UNGPs.

We note we concluded another trip, similar to that described above, in September 2023.

Second, while privacy and safety risks precluded the full publication of our Ethiopia due diligence, we released our first ever annual [human rights disclosure report](#) in mid 2022. The report included our approach to due diligence, insights and actions from our ongoing efforts to identify, prevent, and mitigate human rights risks around the world; UNGP-informed factors to determine countries at risk and a brief overview of our interventions in Ethiopia as outlined below.

You may find pages 65-69 highly relevant. We're excerpting the majority of it here for your convenience:

Integrated Analytical Approaches Countries at Risk

In identified countries (and priority elections), we take a more customized comprehensive due diligence, risk mitigation and response approach — acting quickly to initiate the process to remove content that violates our policies and taking protective measures, including deploying country-specific support. Since 2018, this work has been led by teams with expertise in human rights, hate speech, women and child protection, misinformation, and polarization. Many have lived or worked in high-risk countries and speak relevant languages.

Beginning in 2019, we developed a human rights due diligence process for reviewing and prioritizing countries with the highest risk of offline harm and violence, every six months. To assess long-term conditions on the ground, a cross-functional team of data scientists, political scientists and regional experts review quantitative and qualitative data twice a year drawn from over 60 sources including Varieties of Democracy (V-Dem), Uppsala Conflict Data Program, the United States Holocaust Memorial Museum's Early Warning Project, the Armed Conflict Location & Event Data Project, and the World Bank. This data can include information regarding civic participation and human rights, societal tensions and violence, and the quality of relevant information ecosystems.

UNGP-Informed Factors to Determining Countries at Risk:

Long-term conditions and historical context: We rely on regional experts, platform data and data from more than 60 sources to assess the long-term conditions on the ground. • How much the use of our products could potentially impact a context: We prioritize countries based on a number of factors, including: where our apps have become most central to society, such as in countries where a larger share of people use our products; where there is potential for an increase in offline harms; and where social media adoption has grown. • Current events on the ground: We give special consideration to discrete events that might magnify current societal problems, such as local risk or occurrence of atrocity crimes, polarizing elections, episodes of violence, and COVID-19 vaccination and transmission rates

Guided by the above, we provide specialized support and focus teams on countries most at risk by working to drive human rights to the front of our product, policy, operations, and corporate decision-making. Our focus is

threefold: remove content that violates our policies, respect people's right to free expression, and help to keep people safe both online and offline.

As part of our work, we took the following actions:

- Understand and engage with local contexts and communities to ensure our enforcement accounts for local context. We expanded our global network of third-party fact-checkers, invested significant resources in more than 30 countries with active conflict or societal unrest, and together with UN partners and dozens of local and global NGOs, we developed programming to make online engagement safer.
- Develop and revise policies to prohibit harmful content and behavior by constantly evaluating and refining our policies to address evolving nuances of hate speech, identify groups at heightened risk of violence and human rights abusers, or the potential for rumors and misinformation to contribute to physical harm, particularly in countries where ethnic and religious tensions are present.
- Rapidly enhance our technology and enforcement to help keep our community safe when the risk of impact is greater, i.e. in advance of elections and during periods of heightened unrest. For example, we may reduce or restrict distribution of content from accounts previously found to post content violating our policies, while our teams investigate. Also, we may offer additional features, e.g. providing people in Afghanistan following the Taliban takeover, the ability to lock their profile as an extra layer of privacy, security and protection.
- Improve our moderation across languages by adding more expertise.

Case Study

b. Ethiopia

As of this report's publication, Ethiopia is undergoing a conflict that began in November 2020 between the government of Ethiopia and forces in the northern Tigray region. As the turmoil spreads, the situation remains volatile. Ethiopia is an especially challenging environment to address these issues, in part because there are multiple languages spoken in the country. Meta and its platforms are key avenues for communication in Ethiopia. Diligence: Since early 2020, human rights due diligence for Ethiopia has included field-based information gathering and research; focused stakeholder engagement; and formal due diligence. In 2021, Meta commissioned forward-looking human rights due diligence to help identify existing and prospective human rights risks and inform internal decision-making. We engaged activists, human rights defenders, journalists, civil society groups throughout Ethiopia and the diaspora, adding to the insights gained regularly from human rights groups, NGOs, local civil society organizations, and other regional experts

Action: Using learnings from our due diligence, Meta increased efforts to tackle harmful content (e.g., violence and incitement, hate speech, coordinated inauthentic behavior, misinformation and harm), and addressed elections-related risks and content involving dangerous organizations and individuals. We also:

- Improved and simplified our reporting tools to make it easier for Ethiopian users to report possible violating content, so we can investigate.
- Rolled out a media literacy campaign, aimed at educating and informing people on how to detect potential false news, and ran billboard advertising campaigns across Addis Ababa, the first of its kind in Africa, focused on informing and educating people on how to stay safe online and use social media responsibly.

Partnered with the Center for African Leadership Studies to implement “My Digital World,” a series of live webinars on topics such as online safety, privacy, digital citizenship, news and media literacy.

- Established dedicated reporting channels for specialized international and local human rights and civil society organizations to quickly review problematic content they identify for possible violations.
- Launched a Lock Your Profile feature (as in Myanmar) for Facebook, providing additional safety, privacy and security for our on-the-ground users.
- Increased our investment in proactive detection technology that helps identify violating content such as hate speech before it is reported, including adding in Amharic and Oromo capabilities.
- Hired more Ethiopian nationals with native language skills to monitor and respond to threats in real time, and onboarded more Trusted Partners to provide contextualized advice.

Third, we’ve also publicly shared other updates that address many of your questions. Relevant links include:

[Removing-coordinated-inauthentic-behavior-from-Ethiopia](#)

[Our Approach to Maintaining a Safe Online Environment in Countries at Risk | Meta](#)

[How Facebook is Preparing for Ethiopia's 2021 General Election](#)

[An Update on Our Longstanding Work to Protect People in Ethiopia | Meta](#)

Meta Response to Oversight Board on the Raya Koo case:
[Oversight Board Selects a Case Regarding a Post Discussing the Situation in Ethiopia](#)

Updated Response to Oversight Board on the Raya Koo case:
[Meta Q1 2022 Quarterly Update on the Oversight Board](#)

[Meta Human Rights Report 2022](#) (See pages 65-69)

[Introducing 22 system cards that explain how AI powers experiences on Facebook and Instagram](#)

We do hope you find these useful. We do regret that current litigation makes it impossible to discuss related issues further.

Yours sincerely,



[Redacted Name]

Director, Human Rights Policy

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

CONTACT US



contactus@amnesty.org



+44 (0)20 7413 5500

JOIN THE CONVERSATION



www.facebook.com/amnesty



@Amnesty

BREAKING UP WITH BIG TECH

A HUMAN RIGHTS-BASED ARGUMENT FOR TACKLING BIG TECH'S MARKET POWER

Five Big Tech companies - Google, Meta, Microsoft, Amazon, and Apple - wield extraordinary influence over the infrastructure, services, and norms that shape our online lives. This concentration of power across search, social media, cloud computing, e-commerce, mobile operating systems and more has serious implications for human rights.

This briefing argues that tackling Big Tech's market power is not just about market fairness – it is a human rights imperative. It examines how Big Tech has amassed and sustained powerful positions across digital markets, the human rights harms linked to their dominance, and the risks posed by Big Tech's expansion into generative Artificial Intelligence. It argues that competition law, applied with a human rights lens, can act as a powerful tool for states to implement their human rights obligations under international law.

This briefing calls for a coordinated regulatory response to dismantle harmful concentrations of power and build a more pluralistic, rights-respecting digital ecosystem.