OXFAM DISCUSSION PAPER OCTOBER 2024

RIGHTS AND RESPONSIBILITIES

UNDERSTANDING THE IMPACT OF THE TECH INDUSTRY ON ECONOMIC INEQUALITY

MEG ROGGENSACK, GAWAIN KRIPKE, MICHAEL BORUM, HANA IVANHOE

Digital technologies have the potential to either ameliorate or worsen the dynamics underlying poverty and inequality, depending on how those technologies are designed, developed, deployed, and used, as well as on the degree to which the businesses, and business models behind them, respect the rights of users and workers. This paper recommends changes in corporate and government policies and practices to ensure that the information and communication technology (ICT) industry respects human rights and does not exacerbate poverty and economic inequality across five pillars: access and equity, digital civic space, data use and privacy, automation and the future of work, and governance.

Oxfam Discussion Papers

Oxfam Discussion Papers are written to contribute to public debate and to invite feedback on development and humanitarian policy issues. They are 'work in progress' documents, and do not necessarily constitute final publications or reflect Oxfam policy positions. The views and recommendations expressed are those of the author and not necessarily those of Oxfam.

For more information, or to comment on this paper, email Hana Ivanhoe at hana.ivanhoe@oxfam.org.

www.oxfam.org

OXFAM

CONTENTS

INTRODUCTION

Perhaps more than any other industry, information and communications technologies (ICTs) have an ongoing and ever-increasing impact on peoples' lives, regardless of those people's location, circumstances, or nationality, defying borders and geography and permeating all aspects and sectors of the global economy. This industry has the potential to help reduce poverty and economic inequality and increase respect for and protection of human rights; at the same time, it threatens to entrench that inequality and contribute to the infringement of those rights across countries and a broad range of issues.

So far, the promise of technology to strengthen individual human rights and reduce poverty and economic inequality has gone largely unfulfilled. The sector has failed to preserve digital civic space, automation has adversely impacted workers in multiple ways, and governance failures have allowed tech innovation to result in the concentration of almost inconceivably large amounts of wealth in the hands of the very few. ICTs have been used to disseminate dangerous dis- and misinformation to target and silence vulnerable members of society (like the online hate speech that precipitated the 2019 shooting in El Paso, Texas), trigger election-related violence around the world (like that observed in the lead-up to the January 6, 2021, insurrection in Washington, DC), to fuel ethnic and racial divisions to the point of violent conflict, and even to stoke crimes against humanity, including genocidal conflict.[1]

At the same time, there is arguably more the industry could be doing to help prevent often highly politicized internet shutdowns by authoritarian regimes[2] and the censoring of historically marginalized groups' online speech.

In the workplace, companies have used technology to exploitatively surveil and monitor their own workers to maximize productivity and profit, despite the promises that advances in tech and automation would improve the worker experience. For example, Amazon's first-of-its-kind 'time off task' worker management practice allowed it to gain and maintain an unprecedented online retail market share on the backs of its workers, who now report in alarming numbers that this use of surveillance technology to impose unreasonable productivity standards is harming their health and well-being.[3]

And perhaps more than any other modern industry, the tech industry has relied on monopolistic models to consolidate corporate structures and concentrate wealth and power and has ruthlessly employed cutthroat tax avoidance practices to augment profits.[4]

Despite an endless parade of high-profile scandals and reports of bad corporate behaviour, the governance gap has persisted, with voluntary self-regulation failing to bridge it sufficiently.

In ways unique to the ICT industry, the manner in which digital technologies are designed, developed, deployed, and used – and the businesses and business models behind them – can make an important difference in either fulfilling their promise or making the industry a tool for exploitation and entrenchment of existing poverty and inequality dynamics.

The pace, complexity, and global dimension of technological change are outstripping governments' attempts to regulate, whether through existing policies (which are often misaligned or outdated), new policy mechanisms, or intergovernmental collaborations. Government reliance on private industry for cybersecurity and data management infrastructure presents additional challenges to effective and timely regulation. The situation is further complicated by the actions of repressive regimes seeking to control the tech industry and use it to do their bidding.[5]

To date, the international community has failed to govern or even constrain the tech industry in a meaningful way. Similarly, individual governments have not created meaningful mechanisms to rein in the industry's outsized impact on economic inequality, with the possible exception of recent reforms in the European Union, such as the Digital Services and Digital Markets Acts. Some governments have worked in limited ways to advance freedom online through collaborative efforts such as the Freedom Online Coalition,[6] regulatory initiatives such as the EU's General Data Protection Regulation (GDPR),[7] and emerging mandatory due diligence initiatives. Yet governments have also collaborated on mass surveillance strategies (such as the US PRISM project[8]), ostensibly in service to counterterrorism objectives.

The UN Guiding Principles on Business and Human Rights (UNGPs) – the international community's approach to bridging the governance gap – advise companies to adopt and conduct comprehensive due diligence to ensure that their business practices respect human rights. The B-Tech Project of the UN Office of the High Commissioner for Human Rights (OHCHR) has gone a step further, providing 'authoritative guidance and resources for implementing the UNGPs in the technology space.'[9] Civil society organizations are also doing their part, evaluating the industry's human rights performance across a range of benchmarks, including, but not limited to, Ranking Digital Rights[10] and the Corporate Human Rights Benchmark.[11]

Despite these efforts, the tech industry has largely failed to meet its obligation to respect the human rights of its users and others, and has – with some notable exceptions[12] – shirked accountability for the harms its products have caused, contributed to, or been linked to. ICT companies' human rights efforts, particularly at some of the largest tech companies, are failing to adequately identify and address these core challenges and their implications for users' human rights. United Nations human rights bodies have repeatedly called for the recognition of the right to equitable, affordable, and safe access to the internet, given in part how critical it is to the exercise of other core rights.[13] The right to life and livelihood for marginalized communities, including human rights defenders, is similarly in need of respect and protection and often lacking, such in the face of the automation of work and worker surveillance technology and the misuse and weaponization of mis- and disinformation against vulnerable populations. If not addressed urgently, the industry's persistent failure to employ adequate human rights due diligence practices and uphold digital rights will replicate and reinforce existing inequities and barriers to advancement, further entrenching economic inequality and poverty.[14]

Exacerbating these governmental and corporate governance failures is the concentration of ICT sector ownership in the hands of a small group of tech CEOs and venture capitalists. By reducing or eliminating competition, this situation makes those few corporations themselves gatekeepers of network access and arbiters of user access and terms of service.

All of this is occurring in a sector that is particularly vulnerable to human rights risks. Seventy-one percent of the world's internet users live in countries that are characterized as not free (37%) or only partly free (34%), according to Freedom House. 'In at least 53 countries, users faced legal repercussions for expressing themselves online, often leading to draconian prison terms.'[15]

Recognizing that rights in the digital age will be a growing focus for Oxfam in coming years, the organization has structured its approach and proposals around five pillars: access and equity, digital civic space, data use and privacy, automation and the future of work, and governance. This paper recommends changes in ICT industry policies and practices to help prevent ICT from exacerbating poverty and economic inequality across the five pillars.

FIVE PILLARS OF ICT POLICY

ACCESS AND EQUITY

Equitable and affordable access to digital infrastructure, tools, and online spaces is a fundamental right of all people and is a foundation from which other digital rights derive. Governments, corporations, and their agents must not intentionally inhibit access to or reasonable use of these tools and infrastructure or limit their use by civil society for political or humanitarian purposes. In fact, providing access should be considered a responsibility of duty bearers.

Analysis supported by the ICT industry indicates a positive relationship between digital access and achievement of the Sustainable Development Goals like ending poverty (SDG1) and hunger (SDG2).[16] Research from the International Monetary Fund shows that a 1 percentage-point increase in the share of internet users in the population raises per capita economic growth by as much as 0.4 percentage points in sub-Saharan Africa.[17]

Despite this evidence, 2.7 billion people lack access to the internet.[18] Equitable access is denied across longstanding intersecting lines of marginalization and exclusion. In low- and middle-income countries, for example, mobile phones are the primary way for people to access the internet, accounting for 85% of broadband connections for 3.2 billion people. However, a significant gender gap exists: as of 2021, women were 16% less likely to use the mobile internet than men.[19]

Yet when considering digital access as a channel for promoting human rights or development, it is important to address the multiple subsidiary dimensions of inequality. One framework for analysing barriers and obstacles to digital inclusion consists of five *A*s of technology access: availability, affordability, awareness, accessibility, and ability.[20] Other intersecting axes of exclusion prevent people from accessing digital tools and community. For instance, rural residents are less likely to have access owing to lack of infrastructure, poverty, language barriers, and other factors. In short, digital access is not a simple binary; it has multiple dimensions, including physical, financial, socio-demographic, cultural, institutional, political, and cultural forms of access.[21]

The COVID-19 pandemic, when shutdowns led to a surge in online use, highlighted how critical digital access could be to fulfilling human rights and accessing basic services. For example, ICTs were essential for children and young people in many countries to continue their education; millions of children adapted to online and remote learning. According to UNICEF, however, 'two-thirds of the world's school-age children – or 1.3 billion children aged 3 to 17 years old – do not have internet connection in their homes.'[22] For families unable to switch to online learning, the lack of access has been particularly harmful. ICTs can also provide adults with valuable opportunities to learn new skills and fulfil their own potential.

During the pandemic, the use of ICTs in healthcare, in the form of telemedicine and online counselling, became more prevalent as well. This shift led to an increase in access to medical and mental health services for rural populations, who may lack convenient healthcare infrastructure. Nonetheless, the World Health Organization cites the lack of ICT infrastructure as the primary barrier to wider use of telemedicine.[23]

ICTs can play an important role in community and individual resilience. During shocks and emergencies, ICTs allow individuals to access timely and potentially life-saving information as well as critical healthcare. Any approach to local capacity growth should include the development, training, and use of ICTs that can close temporary gaps in access to health services during acute crises. At the same time, ICTs alone are not an equitable substitute for necessary investments in permanent healthcare infrastructure that is centred on care and focused on optimal patient outcomes.

One of the greatest threats to access: Government shutdowns and censorship

It could be argued that the human rights to freedom of expression and an adequate standard of living effectively necessitate equitable access to the internet in this technology-dominated global economy.[24] Yet a sharp increase in internet shutdowns and censorship has accompanied the trending rise in authoritarianism worldwide. Access Now and the #KeepItOn campaign report that governments and other actors disrupted the internet at least 283 times across 39 countries in 2023, an increase from 201 shutdowns in 2022.[25] These shutdowns in digital access are often accompanied by real-world violence and repression.[26]

In June 2021 the government of Nigeria shut down access to Twitter (now known as X) for eight months after Twitter deleted a post by President Muhammadu Buhari that Twitter claimed violated its terms of service. The post was characterized as fomenting violence against one of Nigeria's main ethnic groups.[27]

It has become increasingly common for certain governments to block internet access entirely or restrict access to specific websites and applications during periods of heightened tension or crisis, as Tanzania reportedly did during its 2020 elections or to silence dissent;[28] ban some mobile applications (Facebook and Twitter are both officially banned in numerous totalitarian states); or censor political or otherwise controversial content. US lawmakers have made efforts to ban the social media platform TikTok over concerns regarding its partial foreign ownership.[29]

Authorities in at least 47 countries have limited users' access to information sources located outside of their borders, arguably infringing on the Universal Declaration of Human Rights, which codifies the right 'to seek, receive, and impart information and ideas through any media and regardless of frontiers.'[30] When governments have cut off internet access, human rights advocates have called for access restoration.[31, 32]

In promoting improved digital access, it is useful to conceive of 'constituencies of access' – the core communities that most need improved access to the digital world or protection of existing access. The gender digital divide is one of the starkest, so women are a critical constituency of access.[33]

Another dimension of access is economic. As economies become increasingly digital and knowledge- and service-based, those who lack sufficient access and skills will be left further behind, with digital divides even widening inequality within and between countries.[34] Improving economic access is about removing the structural barriers that inhibit the world's poorest communities from using ICTs as an engine for creativity, innovation, and economic growth and opportunity.

Cultural access involves ensuring that the diverse peoples of the world have equal access to the vast potential and facility the internet offers. Those who do not share a common language or other key cultural signifiers with the dominant group, such as race, ethnicity, social class, or religious faith, often find their minority status replicated in their digital experiences. The cultural relevance, knowledge, and significance of these populations is rendered effectively invisible, contributing to a perception that the network is more homogeneous in its composition than it really is, and perhaps (albeit unintentionally) perpetuating neocolonial dynamics. Language is a useful way to illustrate this disparity. At present, only 20% of people on Earth speak English as their first language, yet on a global level, as of December 2020, 60.3% of the top 10 million websites were in English. The next most common language in the top five is Russian, at 8.6%, followed by Spanish (4.0%), Turkish (3.5%), and Persian (2.9%).[35]

In these ways and others, inequitable access to ICT platforms leads to economic inequality. While governments must do more to improve equitable access, ICT companies should ensure that they design and deploy those platforms in a manner that encourages rather than discourages equitable access.

DIGITAL CIVIC SPACE

Access alone is important to breaking free from the dynamics of economic inequality that entrench global poverty, but access to the digital civic space in particular must be protected. A cornerstone of functioning democracies, civic space is the set of legal, policy, institutional, and practical conditions nongovernmental actors need to access information, express themselves, associate, organize, and participate in public life.[36] The UN Special Rapporteur on the rights to freedom of peaceful assembly and of association finds digital technology has become integral to the exercise of these rights. By serving as both a tool and an organizing paradigm, digital civil society can advance human rights and innovate for social change. Digital platforms have become crucial tools for mobilization and collective action as well as virtual spaces where marginalized groups that face severe restrictions to operating in physical places can form online assemblies and associations.[37]

At the same time, however, the failure or refusal of the industry to ensure proper content moderation[38] and – above all else – refrain from the use of dangerous algorithms that promote and amplify the most incendiary forms of dangerous speech online has itself contributed to the deterioration of the online civic space by making it an incubator for offline violence. Given the current state of algorithms employed by the leading social media platforms, it is unlikely that more unmoderated expression on platforms is the best solution to the problem of oppression and violent conflict. The lack of moderation and algorithmic integrity can subject marginalized individuals and populations to targeted forms of abuse and intimidation.

To the extent that moderation is valuable, insufficient resources have been invested to account for local contexts and languages. With millions of posts per day on major social platforms, it is impossible to moderate every piece of content. Challenges and problems with over- and undermoderation persist, even with artificial intelligence (whose use is itself problematic for numerous reasons) and other tools to flag potentially problematic content. The humans who conduct moderation are plagued by psychological and emotional trauma as a result of moderating extreme content.

Even more than deficient moderation, the use of opaque and highly secretive algorithms that intentionally and directly amplify incendiary and dangerous speech is perhaps the greatest threat to a free and prospering digital civic space. Social media and communications platforms have developed highly effective algorithms for driving users toward the most polarized, radicalized content to maximize readership clicks and therefore advertising revenues. A Meta whistleblower said, 'Facebook's products harm children, stoke division, and weaken our democracy' because the algorithms favour more controversy, misinformation, extremism, and outrageous content.[39] YouTube is increasingly cited as a cause of political and misogynistic polarization, with algorithms leading viewers into dark conspiracies and toward controversial viewpoints.[40] These highly accessible platforms attract a wide audience of people looking for all sorts of information, which can be dangerous when the algorithm pushes extremist content. Large audiences can become radicalized in ways that have real-life consequences for the political climate. [41]

The so-called democratizing influence of digital spaces – though hailed by many as transformative – is being corrupted and threatens a retreat. The space for people to speak out, organize, and coordinate action against poverty, inequality, and injustice, and hold duty bearers and power holders to account, is shrinking on a global scale.[42] And in recent years, networks and popular platforms have been co-opted and exploited for political or financial gain by state and nonstate actors seeking to undermine liberal democracy and its institutions, press freedoms, and the myriad important functions of a healthy civil society.

The growing prevalence of mis- and disinformation and dangerous speech designed to exclude, intimidate, and silence people, especially women and members of other traditionally marginalized and oppressed groups, is particularly toxic to the online civic space:

> *All over the world, women in politics and journalism experience relentless volumes of online abuse, threats, and gendered disinformation campaigns on social media – and things are even worse for women facing intersectional discrimination and bias on the basis of race, ethnicity, religion, and other factors. These campaigns are designed to discredit, devalue, and delegitimize women's political standing, with the goal of ultimately undermining their ability to participate in civic life.*[43]

Social media and communications platforms must increase their accountability to groups at risk, including the LGBTQ+ community, ethnic minorities, human rights defenders, and women and girls. They can do this by establishing and enforcing strict codes of conduct for users; developing robust and consistent standards for content moderation that detect and respond to defined threats, including all forms of gender-based violence; applying effective sanctions to perpetrators; and reporting transparently to the public on the impact of these initiatives. Technology providers should strengthen or adopt positive measures developing, designing, and using digital technologies to prevent technology-facilitated gender-based violence.[44]

Online Content Leading to Violent Conflict Offline

Dangerous online speech does not just threaten to erode democracy and enable authoritarianism. It also contributes to real-life violence within communities and within and between countries. Meta's social media platform Facebook, for example, has been used to amplify dangerous speech that has been linked to offline violence.

Its algorithms are alleged to have contributed to the escalation of ethnic violence and conflict in Ethiopia. The posting of misinformation and inflammatory information has directly led to violence. In one case, a village predominantly made up of ethnic minorities was reportedly attacked after an inflammatory Facebook post publicly accused its citizens of murder and kidnapping.[45] Unfortunately, tech companies provide little information on the algorithms largely responsible for determining what content a user views, despite a chorus of stakeholder calls for greater algorithmic transparency.[46]

More than perhaps any other industry, the ICT sector is minimally regulated, if not entirely unregulated, and it exerts near monopolistic control over ICT infrastructure, as well as an outsized influence over industry standards and practices. Some countries have taken steps to regulate the industry, while others, such as the United States, have so far provided little government oversight and instead rely more on corporate self-regulation.

The UNGPs state that even where government standards or enforcement are lacking, tech companies are responsible for respecting human rights. There are many ways of preserving the digital civic space that infringe neither on people's right to life and well-being nor on their freedom of expression. In fact, the UNGPs include a mechanism for balancing competing rights in the form of a severity analysis.[47]

Given these platforms' power and potential for harm, their entry into conflict-affected and high-risk areas, characterized by serious human rights violations and severe harm to individuals, requires a heightened level of care and diligence on the part of all companies. In such contexts, ICT companies risk exacerbating conflict and instability, enabling human rights violations, and potentially suffering harms themselves. The consequences can include loss of life, liberty, and livelihoods among community members, employees, suppliers, contractors, and customers, as well as reputational damage, operational interruptions, legal liability, and financial penalties for the business.[48, 49] The UNGPs require a stronger level of review and the dedication of more resources to safety and content moderation in these situations.

Conflict, violence, and rampant human rights abuses hinder economic development and further entrench poverty and economic inequality dynamics.[50]

DATA USE AND PRIVACY

The fundamental human right to privacy,[51] as enshrined in Article 12 of the Universal Declaration of Human Rights, dictates that no one shall be subjected to arbitrary interference with their privacy or correspondence. Yet many users of technology are arguably subject to that very interference by third-party corporate entities that extract users' personal data and monetize it.

Understanding the business model under which digital tools and platforms are provided is critically important to evaluating their human rights risks and impacts.[52] Most ICT products are provided free of cost to users with an explicit goal of creating larger advertising markets and an implicit agreement that user data can be monetized, in a practice popularized by Shoshana Zuboff as 'surveillance capitalism.'[53] In many cases the product or service that users value is not the actual profit-making element of the company; rather, users' personal information is. Information about users' identity is routinely gathered, aggregated, and monetized in various ways by ICT vendors, platforms, and hundreds of other companies, some of which have no visible relationship to the primary service or product.

These transactions occur in an opaque digital ecosystem that raises important questions about control over personal data and individual privacy online. This lack of transparency and, in many contexts, the lack of user control over how personal data is stored, shared, and used carry risks. Digital platform users and consumers have little understanding of exactly what data they are disclosing and what the implications are, but one international survey found 80% of respondents worried about online privacy, with one in four saying they did not trust the internet.[54]

Access to digital tools and communities has many benefits, but the data that users disclose can also be misused to harass, manipulate, oppress, exploit, or simply take unfair advantage, whether by its custodians (a corporation, nonprofit, or government agency) or by others who may have obtained the data illegally through exfiltration or legally through undisclosed third-party agreements with partners or data brokers. To ensure a fair and inclusive digital age, data collection and use must respect the autonomy of individuals by gathering sensitive personal information only when necessary, while being transparent about how this data will be stored, maintained, and used; providing redress for breaches of data security; and providing clear methods for opting out of data collection and for having one's personal data purged from systems on which it is stored. These policies must be presented to users in accessible ways that account for variations in language, ability, education, gender, and other cultural factors that may impact individuals' ability to understand their rights and to ensure their rights are respected.[55]

Many ICT companies' business models encourage excessive retention of users' data as a source of profit, even as they sustain frequent security failures. Governments have proven unable or unwilling to address these deficiencies and have sought to prevent or otherwise limit end-to-end encryption and other security-enhancing protections. Furthermore, numerous governments have cultivated hacking capabilities to exploit vulnerabilities in technologies rather than ensuring they are repaired. It is increasingly common for human rights activists, journalists, and political opposition members to have their devices hacked with spyware that allows attackers to surveil and monitor their online activities.[56]

These assaults on the digital security of civil society occur throughout the world, though they may play out differently depending on the region in which they occur. In conflict zones, the consequences of surveillance and digital attacks can be particularly dire, but many countries where the rule of law is relatively strong also target domestic civil society groups in ways that may violate privacy rights. In Canada, the Quebec police surveilled journalists who were investigating police corruption.[57] The US government's mass surveillance programs target civil society groups from human rights activists to nonprofit medical organizations.[58]

One can argue that individuals may voluntarily sell or loan their data, as a personal asset, to others, such as businesses and nonprofit organizations, for temporary use in a presumably bilateral exchange. The fundamental element of this exchange is consent – permission to collect, store, and use personal data that has been shared. Ideally, consent should be free, specific, informed, unequivocal, and revocable, according to the UN Special Rapporteur on the Right to Privacy.[59] To respect their users' fundamental human right to privacy, companies must ensure that their platform includes a sufficient mechanism for user consent before extracting personal info and that that consent is free, specific, informed, unequivocal, and revocable.

Beyond establishing a mechanism for user consent, data gatherers need to contextualize their efforts and conduct a power analysis of how consent might have unintended impacts on subjects. In general, the study of privacy and consent has allocated too little effort to understand and accommodate the situation of people experiencing poverty or other forms of marginalization. One study found that of 2,823 privacy-related papers published between 2010 and 2020, only 3% (88) focused on marginalized contexts. People who face marginalization in society often have unique privacy-related needs and behaviours that must be recognized and accommodated by researchers and designers of technology. These populations can experience disproportionate harms when their privacy is violated. The calculus about consent is thus very different for people with marginalized identities, and the trade-offs about disclosure and risk require intersectional analysis and remediation.[60,61] For example, the privacy concerns of a person living with HIV, who may risk social stigma, discrimination, or the dissolution of relationships should their HIV status become publicly known without their consent, is quite different from those of a person who does not have to navigate this often-stigmatized characteristic.

AUTOMATION AND THE FUTURE OF WORK

Digital tools and ICTs have already transformed work and workplaces for hundreds of millions of people across the world. The net employment effect is debated, although it is clear that digital technologies have been disruptive while also driving significant economic growth. Automation may increase worker productivity in some ways while also contributing to overall income inequality.[62]

Digital advances and automation of workplaces have displaced workers (particularly middle-income workers) without necessarily producing accompanying gains in productivity.[63] Since the mid-1990s, the share of middle-skill jobs in total employment fell by about 9.5 percentage points in OECD countries, whereas high-skill and lower-wage jobs rose by about 7.5 and 2 percentage points, respectively.[64]

The ICT industry is also pioneering a new era of outsourcing, in which the low-paying, sometimes psychologically traumatizing 'ghost work' functions needed to keep digital platforms running are moved overseas.[65] This is particularly true for content moderation, a trust and safety function, which has increasingly been outsourced as low-pay, low-skill work to the Global South, with devastating results for those workers' mental health and well-being.[66,67] And recent developments in generative artificial intelligence, although outside the scope of this paper, are likely to intensify these trends and dynamics.

One area of particular concern consists of the productivity technologies (including handheld and wearable devices for monitoring and measuring worker movements) being developed and deployed by large employers to manage and even discipline workers. Workers in many environments are feeling intense and increasing pressure to work harder and faster – to remain on task. One report found that 80% of Amazon workers surveyed felt pressured to increase their productivity based on the company's controversial 'Leadership Principles,' which encourage workers to 'work vigorously' and note that 'speed matters.'[68] Workers are evaluated based on the speed at which they work, and when they take breaks, this time is considered 'time off task.' Amazon has invested in software to develop planning models that map out travel routes for order pickers in the warehouse to minimize the time workers spend assembling orders. Analyses of such models show that, too often, they prioritize management-oriented efficiency criteria at the expense of human factors, such as worker health and safety.[69]

New research shows that the use of these surveillance technologies is having significant adverse impacts on Amazon workers:

- Seventy-two percent of Amazon warehouse workers reported 'how fast [they] work' is measured in detail by company technology always or most of the time, whereas only 58% of workers reported this level of monitoring in a recent survey covering the warehousing industry as a whole.
- Seventy-seven percent of Amazon workers reported that technology can 'tell if [they] are actively engaged in [their] work' always or most of the time. Only 47% of workers reported this level of monitoring in a recent survey covering the warehousing industry as a whole.
- Seventy percent of Amazon workers were unable to confirm that the company they work for takes adequate steps to explain how their data is being used.
- More than half (54%) of the Amazon workers surveyed reported that their production rate makes it hard for them to use the bathroom at least some of the time.[70]

Women (particularly Latine and black women) tend to be disproportionately impacted by the use of this worker surveillance and monitoring technology:

> *Women tended to report higher rates of pressure and anxiety about their production rates across both Walmart and Amazon data. When it came to health- and safety-related questions, women at both companies also reported negative impacts at higher rates than men on many questions measuring pain, safety, and health outcomes.*[71]

Other technologies are being introduced to surveil employees for both security and productivity purposes.[72] Known as 'bossware,' these technologies raise human rights concerns around a range of issues, including dignity of work and privacy. As many as 60% of employers report using some kind of tracking software to monitor employees' work, record keystrokes, take screenshots, log time on apps and websites, and other activities. There are few protections from or regulations of bossware.[73] It is crucial to note that simply working in a job does not mean one waives all privacy rights. The misuse of tech tools like worker surveillance devices and algorithmic management tools to suppress and exploit workers offers another example of the potential of an unchecked ICT sector to entrench economic inequality and poverty.

New policies are needed that explicitly consider the needs and rights challenges that have arisen as a result of these emerging uses of technology to exploit workers more broadly. Rather than conceiving of employees as extractive resources, a better model is to support lifelong learning, skills improvement, and vocational training for workers to enhance their productivity, increase their incomes, and advance their careers. This approach is all the more important to support potentially vulnerable people who might otherwise lack privileges and opportunities conducive to such growth.

This training must occur alongside robust labour protection policies and investment in labour rights enforcement mechanisms to ensure that the most vulnerable workers are protected on all fronts. Additionally, wages for any employment should be set at a minimum living-wage level to ensure that workers can thrive and advance through paid employment. Corporate (and governmental) standards must be adopted to ensure that any worker surveillance technology used does not interfere with workers' health and safety or their rights to organize and collectively bargain.

As technological and digital advances enhance employees' ability to complete job-related tasks online, digital remote work can increase workplace diversity and accessibility for employees from traditionally marginalized or vulnerable populations and those who have difficulty accessing traditional workplaces. Digitalization and remote work may have significant and differentiated implications for different genders. For example, remote options can help facilitate work by care providers, who can face mobility and scheduling constraints owing to the often invisible and unpaid care work they undertake. In addition, digitally facilitated remote work options can meaningfully benefit the well-being of employees, particularly those with disabilities.

The enormous growth of the gig economy has also been a function of digital technologies and applications, but to date those innovations have been used largely to exploit workers. Gig workers should enjoy the same worker protections that the law extends to other workers. They should receive a living wage, and their right to unionize should be fully supported by their employers through union neutrality policies and protected by governments through legislative and regulatory protections for freedom of association and collective bargaining rights. As workplaces and employment arrangements continue to evolve, it is important that benefits, including retirement and health insurance, are portable between employers and employment formats.

GOVERNANCE

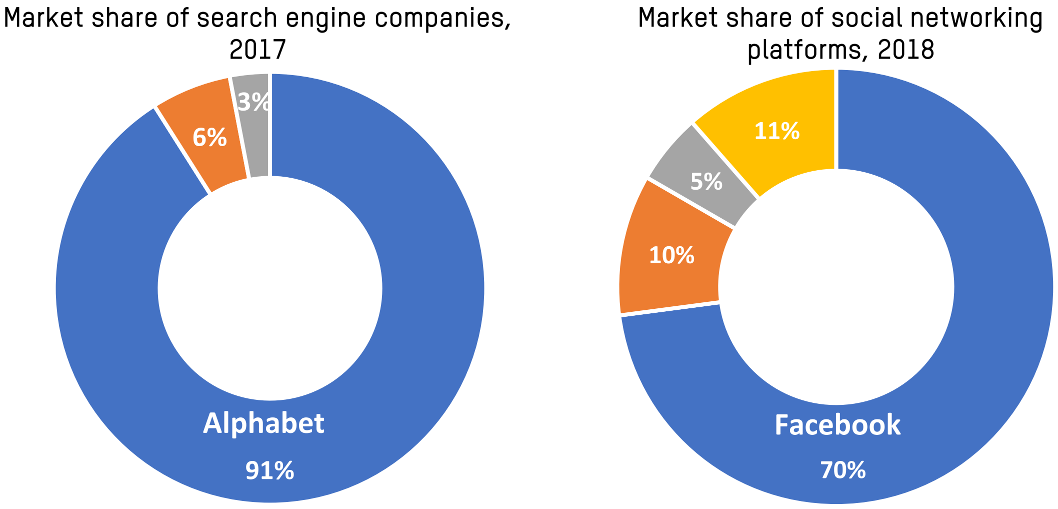
A handful of large and powerful multinational corporations control most of the digital ecosystem, and behind those few corporations is an even smaller group of venture capitalists and other investors pulling the strings. US oversight and regulation have been weak, although these massive tech corporations are increasingly recognized as being 'systemically important' and therefore requiring greater oversight.[74] With few exceptions, US governments across the ideological spectrum have taken a laissez-faire posture that has left the sector with few meaningful regulations, low accountability, and enormous profits that are chronically undertaxed. The most powerful and influential ICT companies are based in the United States, where they are increasingly seeking to exert influence and control over US government decision-makers to ensure continued regulatory paralysis with respect to the ICT industry.[75] The two companies with the highest lobbying expenditures in 2022 were tech companies.[76] Even where policymakers have been bold enough to begin to hold ICT companies accountable for their business models (primarily in the EU to date), the regulations introduced are still quite new and some question how effective their enforcement mechanisms will be.[77] This has had the effect of, once again, reproducing many of the patriarchal, racist, extractive, and environmentally damaging practices of the colonial era and continuing to threaten the human rights of ICT users and people at large.[78]

MARKET CONCENTRATION AND CONSOLIDATION

The tech sector, where assets such as data, software, and other intellectual property matter greatly to economic success, is associated with a tendency toward winner-takes-all dynamics.[79] New technologies alter competition in ways that favour market concentration and domination. In the tech sector, there has been a strong first-mover advantage: companies that can bring a new technology to market earlier have a large, sometimes insurmountable, advantage over later market entrants, even if the first-mover product is inferior.[80] In addition, network effects create powerful obstacles to competition; the larger networks become, the more useful and valuable they are to both owners and users.[81] This phenomenon means that off-network products and services, or alternative networks, have trouble competing with incumbent networks because the hurdle is too high. Other factors also tend to encourage the rise of 'superstar' firms with resilient advantages.

The result is a grievously concentrated ICT industry characterized by near monopoly control by some of the largest companies. Three-quarters of all global online advertisement spending goes to Meta, Alphabet, and Amazon.[82] In addition to consolidating corporate power, monopolies are also bad for consumers. In 2023 the US Federal Trade Commission brought suit against Amazon for using its monopoly power to 'inflate prices, degrade quality, and stifle innovation for consumers and businesses.'[83]According to recent analysis from the Open Markets Institute, as of 2017, the $59.7 billion dollar search engine industry was almost entirely owned and controlled by one company: Alphabet (the parent company of Google), with a staggering 91% market share (Figure 1).[84] Social media platforms are similarly concentrated. Before the entry of TikTok into the market, the three largest platform-owning companies (Meta, Microsoft, and Twitter) controlled 85% of the total market, which produced $34 billion in revenues as of 2018.[85]

Figure 1. Concentration in search engines and social networking platforms



Source: Open Markets Institute. (2024). *Search Engines.* https://concentrationcrisis.openmarketsinstitute.org/industry/search-engines/; Open Markets Institute. (2024). *Social Networking Sites*. https://concentrationcrisis.openmarketsinstitute.org/industry/social-networking-sites/

The erosion of competition is reflected in the increased market power of dominant firms, extraordinary profits that account for a rising share of total corporate profits, and declining business dynamism, especially in industries that are more intensive users of digital technologies.[86] Tech incumbents have a range of strategies at their disposal to reduce or minimize competition. For example, research has shown that 5.3% to 7.4% of US companies acquired between 1989 and 2010 were purchased to kill a competing product.[87] With incumbent companies' large advantages, it is difficult for competitors to gain a foothold, leaving digital markets as effective monopolies.

To spur innovation, ensure proper competition, and combat tendencies toward concentration and consolidation, regulators need to be more interventionist and aggressive.[88] A House Congressional committee investigating competition in digital markets reported, 'Over the past decade, the digital economy has become highly concentrated and prone to monopolization. Several markets investigated by the Subcommittee – such as social networking, general online search, and online advertising – are dominated by just one or two firms. The companies investigated by the Subcommittee – Amazon, Apple, Meta, and Alphabet – have captured control over key channels of distribution and have come to function as gatekeepers.'[89] This tendency toward consolidation and concentration 'has diminished consumer choice, eroded innovation and entrepreneurship in the US economy, weakened the vibrancy of the free and diverse press, and undermined Americans' privacy.'[90]

The increased market concentration and monopolistic behaviour of dominant firms is contributing to growing income inequality and reducing labour's share in the economy in OECD countries.[91] In this way, the ICT sector is playing an outsized role in concentrating wealth and control, not only vertically but also horizontally across geography. Much of the contemporary start-up model consists not of building a company that can grow and win in a competitive market, but rather building a company quickly and then seeking a fast exit by being acquired by one of the large, established ICT companies.[92] The big companies buy smaller companies not only to gain new technologies and businesses, but also to control them and sometimes to suppress them. In any case, when a larger company buys a start-up, it will frequently move operations to Silicon Valley or other established tech centres, exacerbating geographic concentration and inequality.[93]

TAX AVOIDANCE

Tech giants also use a variety of strategies to reduce their tax obligations. Remarkably, given their size and revenues, big tech companies generally pay very low tax rates – lower than most taxpayers. The average effective corporate tax rate is between 19 and 26%,[94] but from 2010 to 2019 'big tech' companies paid an average of between 10.2% and 17.1%.[95] These low tax rates paid partially reflect the kind of creative tax avoidance strategies employed by many multinational companies and the fact that international tax systems have not kept pace with these strategies.[96]

While the bulk of the tech companies' tax avoidance deprives their home countries of revenues, low- and middle-income countries (LMICs) also suffer from lost tax revenue. ActionAid estimates that lost taxes from Alphabet, Facebook, and Microsoft in LMICs total US$2.8 billion – enough revenue to support 879,899 primary school teachers each year in 20 countries across Africa, Asia, and South America.[97]

CONCLUSION

Across the five pillars, ICT companies are failing to respect the human rights of their products' users and global rights-holder populations more broadly. As a result, the industry is entrenching and perpetuating poverty and economic inequality dynamics. In the race to grow the industry, human rights and welfare impacts have been largely neglected to date. But stakeholders are demanding better, and it is time for the industry to do better.

At the moment, the tech companies that dominate the sector face few regulatory or political constraints. Nonetheless, they are obligated by international guidelines to ensure that their actions do not violate the human rights of their users and stakeholders. The UN Guiding Principles on Business and Human Rights and the OECD Guidelines for Multinational Enterprises establish global standards calling on companies to prevent, mitigate, and remedy the human rights impacts of their activities across their value chain; to know and show human rights policies; to conduct human rights due diligence; and to provide effective remedies for human rights impacts.

RECOMMENDATIONS FOR PUBLIC POLICYMAKERS

EQUITABLE ACCESS TO AND PROTECTION OF THE DIGITAL CIVIC SPACE

Governments and international institutions and organizations must do more to protect digital civic space by mandating algorithmic transparency and by moderating online content for safety in a manner that is free of bias and discrimination against marginalized groups and preserves freedom of expression.

Governments must also ensure that they protect their citizens' rights to freedom of expression by ensuring equitable access to the internet and ceasing any and all internet shutdowns or efforts at politically motivated censorship.

AUTOMATION AND THE FUTURE OF WORK

Governments should ensure that all advances in automation and roboticization in the workplace are for the benefit of worker well-being (including health and safety) rather than at the expense of it. In particular, governments must regulate the use of worker surveillance technology to ensure that (i) it is employed only for purposes of protecting workers' own safety (e.g., security cameras in workplaces), (ii) it is fully and transparently disclosed to workers, (iii) workers' consent to the use of surveillance technology is not a requisite condition of work, and (iv) such surveillance is never used to impose or enforce working quotas or productivity standards or as the basis for disciplinary actions.

In addition, governments must protect the right to dignified work that earns workers and their families a living wage and ensure that emerging technologies that automate the workplace do not deprive workers of access to those jobs. While some level of automation is acceptable if it increases physical safety and well-being, governments must balance this with investments in social programs that offset the impacts of displacement caused by automation, including broadening programs that provide workers with the knowledge, skills, and abilities needed to adapt to a changing work environment.

GOVERNANCE: ANTITRUST AND TAX AVOIDANCE

Policymakers should enforce existing policies that limit anticompetitive behaviour, while simultaneously identifying opportunities to strengthen anticompetitive policy to better reflect new market realities. Governments must break up private monopolies and prevent ICT companies from becoming too large and dominating their sectors. Breaking up monopolies and preventing monopolistic mergers in a manner that prevents tech companies from becoming too large is vital to addressing extreme inequality. Prominent past breakups in other industries have led to explosions of innovation and growth, and antimonopoly enforcement has generally been shown to reverse many of the harms of monopoly by raising wages, increasing employment, and lowering prices.[98] The recent Department of Justice lawsuit against Apple alleging its iPhone practices violate antitrust laws,[99] followed by the landmark finding in the antitrust case against Google, stating that the company is a 'monopolist,' are promising steps in the right direction. Nonetheless, even more aggressive antitrust actions are needed from regulatory authorities in the US and beyond in order to combat monopolistic tendencies and the economic inequality they perpetuate.[100]

Governments must also address the collapse in corporate taxation that has come to characterize the ICT sector. Addressing corporate taxation is essential to tackling the accumulation of extreme wealth and to supporting inequality-busting services and programs. To prevent companies taking advantage of regulatory loopholes to reduce their tax liability, policymakers should close loopholes, end corporate tax secrecy by ensuring all multinational ICT companies publish tax transparency reports, and reform tax policies to ensure that corporations pay their fair share of taxes in the jurisdictions where their economic activity takes place.[101]

RECOMMENDATIONS FOR INDUSTRY

STRENGTHENED HUMAN RIGHTS DUE DILIGENCE

Companies should adopt or strengthen existing human rights due diligence policies and practices that apply across departments, markets, products, and operations. In particular, those policies and practices should prioritize entry into new markets or delivery of new or expanded services, operations in fragile and conflict settings, and the potential for risks arising from design use and misuse (including the use of algorithms and other forms of artificial intelligence).

Meaningful and effective human rights due diligence requires the following:

- A comprehensive plan for the administration of human rights due diligence
- The regular conduct of human rights impact assessments, including
    - consultation with relevant rights holders
    - publication of all findings of the impact assessments
    - acknowledgement by the company of the degree to which they have caused, contributed to, or been directly linked to human rights risks
    - an action plan for preventing future risks, mitigating existing risks, and remedying any identified rights violations
- A fully anonymized grievance mechanism accessible by all potentially impacted rights holders and available in all relevant languages to ensure redress for grievance to victims
- Enhanced human rights due diligence when circumstances warrant, such as in fragile or conflict sensitive settings.

In line with their human rights due diligence journeys, companies should invest more in stakeholder engagement, particularly with respect to reaching potential users who experience barriers to access and identifying and addressing the human rights concerns of traditionally marginalized or oppressed groups. At a minimum, stakeholder engagement should create opportunities to shape company tools and policies for addressing risks and barriers.

CORPORATE LEADERSHIP ON HUMAN RIGHTS

Senior executive management teams and the boards of directors of technology companies should oversee and guide efforts to ensure human rights-respecting business practices throughout company operations and at all stages of their product's life cycle (design, deployment, and use), supported by a dedicated human rights team with sufficient authority and resources to function effectively.

This approach can be achieved meaningfully and effectively through various mechanisms:

- Executives' key performance indicators should include policies that respect the human rights of users' and other beneficiary communities rather than just ad sales and other product performance indicators.
- Resource investment in a given market should be correlated to the level of identified human rights risk rather than to commercial risk or level of regulatory sophistication.
- Corporate structures should integrate interrelated departments like human rights, legal compliance, and trust and safety on the one hand, and product development and ad sales on the other, so that human rights due diligence policies are integrated into and throughout other departmental policies. These efforts should include actively monitoring the company's business footprint, partnerships, and user base.

MEANINGFUL TRANSPARENCY

ICT companies should regularly publish detailed public reports on all matters relevant to rights holders and other stakeholders and assessments of how these concerns have informed business decisions and how these in turn are reflected in day-to-day operations. This reporting should include the following:

- publication of the complete findings of human rights impact assessments (including how company activities are causing, contributing to, or leading to various rights risks, as outlined above)
- the types, forms, and purpose of the various algorithms and other forms of artificial intelligence employed in furtherance of their business models
- content moderation processes and responses to enhance safety, particularly for at-risk users
- information on their public advocacy efforts to promote online freedoms and to support multisector efforts to address challenges of equity and access
- tax transparency (including country-by-country reporting)
- post-crisis assessments, including findings and recommended changes in business policies and practices

FREEDOM OF ASSOCIATION AND COLLECTIVE BARGAINING

To address concerns about automation and the future of work (including for gig economy and content moderation workers), companies must respect workers' collective bargaining rights. Companies should commit to maintaining a neutral stance on workers' union activity and allow freedom of association for workers, as called for in the United Nations Global Compact and Universal Declaration of Human Rights. In line with that, companies should

- Commit publicly to maintain a neutral stance on union activity (including refraining from union busting or intimidation in any form), and state their commitment to respect freedom of association and collective bargaining rights in relevant company policies.
- Agree to recognize, engage, and negotiate in good faith with any and all duly elected labour unions and to consult those labour unions or other worker organizations legitimately representing workers on any other commitments the company makes and implements in furtherance of those commitments.

NOTES

[1] L. Rainie, J. Anderson, and J. Albright. (2017). *The Future of Free Speech, Trolls, Anonymity and Fake News Online*. Pew Research Center. https://www.pewresearch.org/internet/2017/03/29/the-future-of-free-speech-trolls-anonymity-and-fake-news-online/

[2] The following paper offers some fairly comprehensive recommendations for industry along these lines: S. Feldstein. (2022). *Government Internet Shutdowns Are Changing. How Should Citizens and Democracies Respond?* Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2022/03/government-internet-shutdowns-are-changing-how-should-citizens-and-democracies-respond?lang=en

[3] Oxfam America. (2024). *At Work and under Watch: Surveillance and Suffering at Amazon and Walmart Warehouses*. https://www.oxfamamerica.org/explore/research-publications/at-work-and-under-watch/

[4] J. Tankersley. (9 October 2019). 'Tech Giants Shift Profits to Avoid Taxes. There's a Plan to Stop Them.' *New York Times*. https://www.nytimes.com/2019/10/09/us/politics/tech-giants-taxes-oecd.html

[5] A. Shahbaz and A. Funk. (2021). *Freedom on the Net 2021: The Global Drive to Control Big Tech*. Freedom House. https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech

[6] Freedom Online Coalition. (2024). *Aims and Priorities*. Freedom Online Coalition. Accessed 1 October 2024. https://freedomonlinecoalition.com/aims-and-priorities/#priorities

[7] General Data Protection Regulation. (2023). *Complete Guide to GDPR Compliance*. https://gdpr.eu

[8] R. Lempert. (13 June 2013). *PRISM and Boundless Informant: Is NSA Surveillance a Threat?* Brookings Institution. https://www.brookings.edu/articles/prism-and-boundless-informant-is-nsa-surveillance-a-threat/

[9] United Nations Office of the High Commissioner for Human Rights (UN OHCHR). (2024). *B-Tech Project*. https://www.ohchr.org/en/business-and-human-rights/b-tech-project

[10] Ranking Digital Rights. (4 May 2022). *The 2022 Big Tech Scorecard*. https://rankingdigitalrights.org/bts22/

[11] World Benchmarking Alliance. (2023). *Corporate Human Rights Benchmark*. https://www.worldbenchmarkingalliance.org/corporate-human-rights-benchmark/#:~:text=The%20Corporate%20Human%20Rights%20Benchmark,they%20respond%20to%20serious%20allegations.

[12] The Global Network Initiative (GNI) was the first tech-focused multistakeholder initiative to assess companies on their efforts to integrate human rights principles and to assess progress through specific case examples. GNI, however, is limited in scope and focuses only on the specific threats to freedom of expression and privacy posed by government law enforcement requests to ICT companies to, for example, curtail service, remove content, or surveil users. Global Network Initiative. (2023). *About GNI*. https://globalnetworkinitiative.org/about-gni/

[13] See, for example, UN OHCHR. (10 March 2023). It May be Time to Reinforce Universal Access to the Internet as a Human Right, Not Just a Privilege, High Commissioner Tells Human Rights Council. https://www.ohchr.org/en/news/2023/03/it-may-be-time-reinforce-universal-access-internet-human-right-not-just-privilege-high

[14] A. Abrougui, J. Dheere, N. Maréchal, Z. Rogoff, J. Rydzak, V. Wessenauer, and J. Zhang. (27 April 2022) *Key Findings from the 2022 RDR Big Tech Scorecard*. Ranking Digital Rights. https://rankingdigitalrights.org/mini-report/key-findings-2022/

[15] A. Shahbaz, A. Funk, and K. Vesteinsson. (2022). *Countering an Authoritarian Overhaul of the Internet*. Freedom House. https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet

[16] Global Enabling Sustainability Initiative (GeSI). (17 July 2018). *A Strong and Positive Link*. Digital Access Index. https://digitalaccessindex-sdg.gesi.org/a-strong-and-positive-link/

[17] M. García-Escribano. (29 June 2020). *Low Internet Access Driving Inequality*. International Monetary Fund blog. https://www.imf.org/en/Blogs/Articles/2020/06/29/low-internet-access-driving-inequality

[18] International Telecommunication Union (ITU). (16 September 2022). *Internet surge slows, leaving 2.7 billion people offline in 2022*. Press release. https://www.itu.int/en/mediacentre/Pages/PR-2022-09-16-Internet-surge-slows.aspx

[19] M. Shanahan. (22 June 2022). *The Mobile Gender Gap Report 2022*. Mobile for Development (GSMA). https://www.gsma.com/r/wp-content/uploads/2022/06/The-Mobile-Gender-Gap-Report-2022.pdf

[20] Roberts, T., and K. Hernandez. (2019). 'Digital Access Is Not Binary: The 5 "A"s of Technology Access in the Philippines.' *Electronic Journal of Information Systems in Developing Countries*, 85, e12084. https://doi.org/10.1002/isd2.12084

[21] N. Williams. (2022). 'Overview on Global Digital Divide.' *Global Journal of Technology and Optimization*, 13(1): 278. https://www.hilarispublisher.com/open-access/overview-on-global-digital-divide.pdf

[22] UNICEF and ITU. (2020). *How Many Children and Young People Have Internet Access at Home? Estimating Digital Connectivity during the COVID-19*. https://data.unicef.org/resources/children-and-young-people-internet-access-at-home-during-covid19/

[23] World Health Organization. (2010). Telemedicine: Opportunities and Developments in Member States.

[24] United Nations. (1948). *Universal Declaration of Human Rights*, Articles 19 and 25. https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf

[25] Access Now. (2024). #KeepItOn. https://www.accessnow.org/campaign/keepiton/

[26] Z. Rosson, F. Anthonio, and C. Tackett. (2023). *Weapons of Control, Shields of Impunity: Internet Shutdowns in 2022*. Access Now. https://www.accessnow.org/wp-content/uploads/2023/05/2022-KIO-Report-final.pdf

[27] J. Beaubien. (9 June 2021). 'Twitter Remains Shut Down In Nigeria After Deleting President's Tweet.' NPR. https://www.npr.org/2021/06/09/1004862371/twitter-remains-shut-down-in-nigeria-after-deleting-presidents-tweet

[28] Giles, C., and P. Mwai. (14 January 2021). 'Africa internet: Where and How Are Governments Blocking It?' BBC News. https://www.bbc.com/news/world-africa-47734843

[29] Despite this attention from US lawmakers, Tik Tok maintains that its parent company, ByteDance, is majority owned by international investors. S. Maheshwari and D. McCabe. (23 April 2024). 'Congress Passed a Bill That Could Ban TikTok. Now Comes the Hard Part.' *New York Times*. https://www.nytimes.com/2024/04/23/technology/bytedance-tiktok-ban-bill.html

[30] A. Shahbaz, A. Funk, P. Friedrich, K. Vesteinsson, G. Baker, C. Grothe, et al., eds. (2022). *Freedom on the Net 2022: Countering an Authoritarian Overhaul of the Internet*. Freedom House. https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf

[31] Human Rights Watch. (31 March 2020). *End Internet Shutdowns to Manage COVID-19*. https://www.hrw.org/news/2020/03/31/end-internet-shutdowns-manage-covid-19

[32] Human Rights Watch. (19 June 2020). *Myanmar: End World's Longest Internet Shutdown*. https://www.hrw.org/news/2020/06/19/myanmar-end-worlds-longest-internet-shutdown

[33] Oxfam Novib. (31 October 2019). 'Human Rights in a Digital Age: What Should Oxfam Novib's Role Be?' Summary of discussions and working group recommendations.

[34] M. García-Escribano. (29 June 2020). *Low Internet Access Driving Inequality*. International Monetary Fund blog. https://www.imf.org/en/Blogs/Articles/2020/06/29/low-internet-access-driving-inequality

[35] W3Techs. (December 2020). *Usage Statistics of Content Languages for Websites*. https://w3techs.com/technologies/overview/content_language

[36] Organisation for Economic Co-operation and Development (OECD). (2022). *The Protection and Promotion of Civic Space: Strengthening Alignment with International Standards and Guidance*. https://doi.org/10.1787/d234e975-en

[37] International Center for Non-profit Law. (June 2019). *Assembly and Association in the Digital Era*. https://www.icnl.org/post/analysis/assembly-and-association-in-the-digital-era

[38] Bloomberg, among others, noted an industry-wide slowdown in content moderation efforts in 2023: D. Alba. (26 December 2023). *Social Media Companies' Moderation Efforts Lost Steam in 2023*. Bloomberg. https://www.bloomberg.com/news/newsletters/2023-12-26/social-media-companies-moderation-efforts-lost-steam-in-2023

[39] K. Hao. (5 October 2021). 'The Facebook Whistleblower Says Its Algorithms Are Dangerous. Here's Why.' *MIT Technology Review*. https://www.technologyreview.com/2021/10/05/1036519/facebook-whistleblower-frances-haugen-algorithms/

[40] M. Fisher and A. Taub. (11 August 2019). 'How YouTube Radicalized Brazil.' *New York Times*. https://www.nytimes.com/2019/08/11/world/americas/youtube-brazil.html

[41] Ibid.

[42] A. Shahbaz, A. Funk, P. Friedrich, K. Vesteinsson, G. Baker, C. Grothe, et al., eds. (2022). *Freedom on the Net 2022: Countering an Authoritarian Overhaul of the Internet*. Freedom House. https://freedomhouse.org/sites/default/files/2022-10/FOTN2022Digital.pdf

[43] She Persisted. (2024). *The Problem*. https://she-persisted.org/the-problem/

[44] Irish Consortium on Gender Based Violence. (2023). *Technology and Gender Based Violence: Risks and Opportunities*. https://www.gbv.ie/wp-content/uploads/2023/03/CSW67-Technology-and-Gender-Based-Violence-Risks-and-Opportunities.pdf

[45] A. Cornish, C. Donevan, and A. Bior. (11 October 2021). 'Facebook Is under New Scrutiny for Its Role in Ethiopia Conflict.' NPR. https://www.npr.org/2021/10/11/1045084676/facebook-is-under-new-scrutiny-for-its-role-in-ethiopias-conflict

[46] A. Abrougui, J. Dheere, N. Maréchal, Z. Rogoff, J. Rydzak, V. Wessenauer, and J. Zhang. (27 April 2022) *Key Findings from the 2022 RDR Big Tech Scorecard*. Ranking Digital Rights. https://rankingdigitalrights.org/mini-report/key-findings-2022/

[47] J. Vaughan. (9 December 2021). 'Human Rights Assessments: Identifying Risks, Informing Strategy.' *BSR*. https://www.bsr.org/en/reports/human-rights-assessments-identifying-risks-informing-strategy

[48] J. Easterday. (2022). Conflict-Sensitive Human Rights Due Diligence for ICT Companies: Guidelines and Toolkit for Corporate Human Rights Practitioners. JustPeace Labs and BSR. https://www.bsr.org/reports/BSR-JPL-Report-Toolkit-Dec-2022.pdf

[49] BSR. (2021). *Business in Conflict-Affected and High-Risk Contexts*. https://www.bsr.org/reports/BSR-Business-in-Conflict-Affected-High-Risk-Contexts-Report.pdf

[50] E. Dabla-Norris, K. Kochhar, N. Suphaphiphat, F. Ricka, and E. Tsounta. (2015). *Causes and Consequences of Income Inequality: A Global Perspective.* https://www.imf.org/external/pubs/ft/sdn/2015/sdn1513.pdf

[51] The international NGO Privacy International defines privacy as 'a fundamental right, essential to autonomy and the protection of human dignity, serving as the foundation upon which many other human rights are built. . . . The rules that protect privacy give us the ability to assert our rights in the face of significant power imbalances. [It] is an essential way we seek to protect ourselves and society against arbitrary and unjustified use of power, by reducing what can be known about us and done to us, while protecting us from others who may wish to exert control. Privacy is essential to who we are as human beings, and we make decisions about it every single day. . . . [It] is an important element of giving us control over who knows what about us.' Privacy International. (2024). *Privacy*. https://privacyinternational.org/learn/privacy

[52] UN OHCHR. (2023). *Human Rights Risks In Tech: Engaging and Assessing Human Rights Risks Arising from Technology Company Business Models*. https://www.ohchr.org/sites/default/files/documents/issues/business/b-tech/BTech-Institutional-Investor-Business-Models-Tool.pdf

[53] S. Zuboff. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs. https://www.hachettebookgroup.com/titles/shoshana-zuboff/the-age-of-surveillance-capitalism/9781610395694/?lens=publicaffairs

[54] R. Muggah. (8 September 2021). *Digital Privacy Comes at a Price. Here's How to Protect It*. World Economic Forum blog. https://www.weforum.org/agenda/2021/09/how-to-protect-digital-privacy/

[55] To date, the most ambitious and far-reaching data protection policy has been the European Union's General Data Protection Regulation (GDPR), which went into effect in 2018. It seeks to balance the practical needs of businesses and government with the importance of privacy and data protection, with a stronger emphasis on the latter. Its human-centric reforms include true consent, easy-to-understand agreements and breach notifications, retention of preexisting rights, data portability, and the right to opt out of profiling. Access Now considers the GDPR to be 'one of the strongest frameworks currently in place to protect personal data and serves as a model for regulation around the world,' though Access Now raised the alarm in 2020 – two years after the rule took effect – over weak implementation and enforcement. See, e.g., Access Now. (2023). *Five Years under the EU GDPR: Becoming an Enforcement Success*. https://www.accessnow.org/wp-content/uploads/2023/05/GDPR-5-Year-report-2023.pdf

[56] UN OHCHR. (19 July 2021). Use of Spyware to Surveil Journalists and Human Rights Defenders: Statement by UN High Commissioner for Human Rights Michelle Bachelet. Press release. https://www.ohchr.org/en/2021/07/use-spyware-surveil-journalists-and-human-rights-defendersstatement-un-high-commissioner

[57] Ibid.; in response, a law was passed in 2017 in Canada to protect journalistic sources. Canada, Justice Laws Website. (2017). 'Journalistic Sources Protection Act.' https://laws-

lois.justice.gc.ca/eng/annualstatutes/2017_22/FullText.html#:~:text=It%20allows%20journalists%20to%20not,public%20interest%20in%20preserving%20the

[58] Edward Snowden is an American (now a naturalized Russian) and former computer intelligence consultant who in 2013 leaked highly classified information from the US National Security agency that revealed numerous global surveillance programs run by government entities with the cooperation of telecommunications companies. Wikipedia. (2024). *Edward Snowden*. https://en.wikipedia.org/wiki/Edward_Snowden

[59] A. Brian Nougrères. (20 July 2022). *Principles Underpinning Privacy and the Protection of Personal Data*. Report to the United Nations General Assembly. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N22/594/48/PDF/N2259448.pdf?OpenElement

[60] S. Sannon and A. Forte. (July 2022). 'Privacy Research with Marginalized Groups: What We Know, What's Needed, and What's Next.' *Proceedings of the ACM Human-Computer Interaction*, 6(CSCW): 1–33. https://arxiv.org/pdf/2206.15037.pdf

[61] Oxfam has established institutional policy in the area of data use and privacy which is aligned with a feminist, rights-based approach and with extensive published knowledge focused on the practice of aid delivery, safe programming, and program evaluation. Some policies are quite recent, while others have been established for several years. These include the Oxfam Biometric and Foundational Identity Policy (2021), One Oxfam Digital Safeguarding Policy (2020), Oxfam Data Protection Policy (2018), and Oxfam Responsible Program Data Policy (2015). The Biometric and Foundational Identity Policy clearly emphasizes the necessity of careful design, planning, risk assessment, data protection, and accountability and further clarifies what the organization will not do. This policy is most consistent with policies supported by other advocacy organizations working in this space and sets a reasonably strong standard for Oxfam moving forward.

[62] S. Lohr. (11 January 2022). 'Economists Pin More Blame on Tech for Rising Inequality.' *New York Times*.

[63] Ibid.

[64] Z. Qureshi. (2021). *Technology, Growth, and Inequality: Changing Dynamics in the Digital Era*. Global Working Paper 152. Brookings Institution. https://www.brookings.edu/wp-content/uploads/2021/02/Technology-growth-inequality_final.pdf

[65] M. L. Gray and S. Suri. (2019). *Ghost Work*. Harper Business. https://ghostwork.info/

[66] B. Perrigo. (18 January 2023). 'Exclusive: OpenAI Used Kenyan Workers on Less Than $2 Per Hour to Make ChatGPT Less Toxic.' *Time Magazine*. https://time.com/6247678/openai-chatgpt-kenya-workers/

[67] C. Kimeu. (7 June 2023). '"A Watershed": Meta Ordered to Offer Mental Health Care to Moderators In Kenya.' *Guardian*. https://www.theguardian.com/global-development/2023/jun/07/a-watershed-meta-ordered-to-offer-mental-health-care-to-moderators-in-kenya

[68] M. Jabsky and C. Obernauer. (16 October 2019). *Time Off Task: Pressure, Pain, and Productivity at Amazon*. Report, New York Committee for Occupational Safety and Health. https://media.business-humanrights.org/media/documents/files/documents/amazon_worker_report_10_15.pdf

[69] Ibid.

[70] Oxfam America. (2024). *At Work and under Watch: Surveillance and Suffering at Amazon and Walmart Warehouses*. https://www.oxfamamerica.org/explore/research-publications/at-work-and-under-watch/

[71] Ibid., p. 26.

[72] B. Cyphers and K. Gullo. (30 June 2020). *Inside the Invasive, Secretive 'Bossware' Tracking Workers*. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2020/06/inside-invasive-secretive-bossware-tracking-workers

[73] T. Klosowski. (6 June 2022). 'There's (Probably) Nothing You Can Do about the New Bossware That's Spying on You.' *New York Times*. https://www.nytimes.com/wirecutter/blog/what-to-do-about-bossware-employee-monitoring/

[74] S. Lohr. (10 December 2022). 'To Rein in Big Tech, Europe Looked beyond Lawsuits. Will the U.S. Follow?' *New York Times*. https://www.nytimes.com/2022/12/10/business/big-tech-antitrust-rules.html

[75] E. Birnbaum. (24 January 2022). 'Tech Spent Big on Lobbying Last Year.' *Politico.* https://www.politico.com/newsletters/morning-tech/2022/01/24/tech-spent-big-on-lobbying-last-year-00001144

[76] Oxfam. (2024). *Inequality, Made in America: How Corporate America Is Fueling our Inequality Crisis*. https://www.oxfamamerica.org/explore/research-publications/inequality-made-in-america/

[77] See, e.g., European Commission. (2024). *The Digital Services Act Package*. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

[78] Oxfam and McGill University Institute for Gender, Sexuality and Feminist Studies/Institute for Health and Social Policy (IGSF/IHSP). (July 2022). *Rights in a Digital Age*. Policy Compendium (internal Oxfam document).

[79] Z. Qureshi. (2021). *Technology, Growth, and Inequality: Changing Dynamics in the Digital Era*. Global Working Paper 152. Brookings Institution. https://www.brookings.edu/wp-content/uploads/2021/02/Technology-growth-inequality_final.pdf

[80] Corporate Finance Institute. (8 July 2020). *First Mover Advantage*. https://corporatefinanceinstitute.com/resources/management/first-mover-advantage/#:~:text=Technology%20leadership,establish%20an%20absolute%20cost%20advantage.

[81] Andrew Beattie. (30 January 2023). 'Understanding First Mover Advantage.' *Investopedia*. https://www.investopedia.com/articles/investing/111016/understanding-first-mover-advantage.asp#:~:text=So%20learning%2C%20size%20and%20access,the%20total%20user%20base%20grows.

[82] Oxfam. (2024). *Inequality Inc.: How Corporate Power Divides Our World and the Need for a New Era of Public Action*. https://oi-files-d8-prod.s3.eu-west-2.amazonaws.com/s3fs-public/2024-01/Davos%202024%20Report-%20English.pdf

[83] Ibid.; US Federal Trade Commission. (26 September 2023). *FTC Sues Amazon for Illegally Maintaining Monopoly Power*. Press release. https://www.ftc.gov/news-events/news/press-releases/2023/09/ftc-sues-amazon-illegally-maintaining-monopoly-power

[84] Open Markets Institute. (2024). *Search Engines*. https://concentrationcrisis.openmarketsinstitute.org/industry/search-engines/

[85] Open Markets Institute. (2024). *Social Networking Sites*. https://concentrationcrisis.openmarketsinstitute.org/industry/social-networking-sites/

[86] Z. Qureshi. (2021). *Technology, Growth, and Inequality: Changing Dynamics in the Digital Era*. Global Working Paper 152. Brookings Institution. https://www.brookings.edu/wp-content/uploads/2021/02/Technology-growth-inequality_final.pdf

[87] C. Cunningham, F. Ederer, and S. Ma. (2021). 'Killer Acquisitions.' *Journal of Political Economy*, 129(3), February. https://doi.org/10.1086/712506.

[88] E. Argentesi, P. Buccirossi, E. Calvano, T. Duso, A. Marrazzo, and S. Nava. (2019). *Merger Policy in Digital Markets: An Ex-Post Assessment*. DIW Berlin Discussion Paper No. 1836. Deutsches Institut für Wirtschaftsforschung (DIW). https://ssrn.com/abstract=3501501

[89] Subcommittee on Antitrust, Commercial, and Administrative Law of the Committee on the Judiciary of the House of Representatives, US Congress. (2021). *Investigation of Competition in Digital Markets*. https://www.govinfo.gov/content/pkg/CPRT-117HPRT47832/pdf/CPRT-117HPRT47832.pdf

[90] Ibid.

[91] D. Autor, D. Dorn, L. F. Katz, C. Patterson, and J. V. Reenen. (2020). 'The Fall of the Labor Share and the Rise of Superstar Firms.' *Quarterly Journal of Economics*, 135(2), 645–709. https://academic.oup.com/qje/article/135/2/645/5721266?login=false

[92] Silicon Valley Bank. (2019). *US Startup Outlook 2019*. https://www.svb.com/globalassets/library/uploadedfiles/content/trends_and_insights/reports/startup_outlook_report/us/svb-suo-us-report-2019.pdf

[93] Kenan Institute. (11 August 2021). *Big Tech, Bigger Regional Inequality?* https://kenaninstitute.unc.edu/kenan-insight/big-tech-bigger-regional-inequality/

[94] D. Bunn and G. Watson. (2 April 2021). *U.S. Effective Corporate Tax Rate Is Right in Line with Its OECD Peers*. Tax Foundation blog. https://taxfoundation.org/us-effective-corporate-tax-rate-oecd-peers/

[95] Fair Tax Mark. (2019). *The Silicon Six and Their $100 Billion Global Tax Gap*. https://fairtaxmark.net/wp-content/uploads/2019/12/Silicon-Six-Report-5-12-19.pdf

[96] A. Borrett. (18 February 2021). *Consensus Is Emerging on How to Tax Big Tech*. Tech Monitor. https://techmonitor.ai/leadership/strategy/consensus-emerging-on-taxing-big-tech-companies

[97] ActionAid. (26 October 2020). *$2.8bn 'Tax Gap' Exposed by ActionAid Research Reveals Tip of the Iceberg of 'Big Tech's Big Tax Bill' in the Global South*. https://actionaid.org/news/2020/28bn-tax-gap-exposed-actionaid-research-reveals-tip-iceberg-big-techs-big-tax-bill-global

[98] Oxfam. (2024). *Business at an Inhuman Scale: How America's Biggest Retailers Are Driving Its Economic Inequality Crisis*. https://www.oxfamamerica.org/explore/research-publications/business-at-an-inhuman-scale/

[99] D. McCabe and T. Mickle. (21 March 2024). 'U.S. Justice Dept. Sues Apple, Claiming iPhone Monopoly in Antitrust Case.' *New York Times.* https://www.nytimes.com/2024/03/21/technology/apple-doj-lawsuit-antitrust.html

[100] D. McCabe. (5 August 2024). '"Google Is a Monopolist," Judge Rules in Landmark Antitrust Case.' *New York Times*. https://www.nytimes.com/2024/08/05/technology/google-antitrust-ruling.html

[101] Oxfam. (2024). *Business at an Inhuman Scale: How America's Biggest Retailers Are Driving Its Economic Inequality Crisis*. https://www.oxfamamerica.org/explore/research-publications/business-at-an-inhuman-scale/

Oxfam Discussion Papers

Oxfam Discussion Papers are written to contribute to public debate and to invite feedback on development and humanitarian policy issues. They are 'work in progress' documents, and do not necessarily constitute final publications or reflect Oxfam policy positions. The views and recommendations expressed are those of the author and not necessarily those of Oxfam.

For more information, or to comment on this paper, email Hana Ivanhoe at hana.ivanhoe@oxfam.org.

The information in this publication is correct at the time of going to press.

Published by Oxfam GB for Oxfam International in October 2024. DOI: 10.21201/2024.000040

Oxfam GB, Oxfam House, John Smith Drive, Cowley, Oxford, OX4 2JY, UK.

OXFAM

Oxfam is an international confederation of 21 organizations, working with its partners and allies, reaching out to millions of people around the world. Together, we tackle inequalities to end poverty and injustice, now and in the long term – for an equal future. Please write to any of the agencies for further information or visit www.oxfam.org.

Oxfam America (www.oxfamamerica.org)
Oxfam Aotearoa (www.oxfam.org.nz)
Oxfam Australia (www.oxfam.org.au)
Oxfam-in-Belgium (www.oxfamsol.be)
Oxfam Brasil (www.oxfam.org.br)
Oxfam Canada (www.oxfam.ca)
Oxfam Colombia (www.oxfamcolombia.org)
Oxfam France (www.oxfamfrance.org)
Oxfam Germany (www.oxfam.de)
Oxfam GB (www.oxfam.org.uk)
Oxfam Hong Kong (www.oxfam.org.hk)
Oxfam IBIS (Denmark) (www.oxfamibis.dk)
Oxfam India (www.oxfamindia.org)
Oxfam Intermón (Spain) (www.oxfamintermon.org)
Oxfam Ireland (www.oxfamireland.org)
Oxfam Italy (www.oxfamitalia.org)
Oxfam Mexico (www.oxfammexico.org)
Oxfam Novib (Netherlands) (www.oxfamnovib.nl)
Oxfam Québec (www.oxfam.qc.ca)
Oxfam South Africa (www.oxfam.org.za)
KEDV (www.kedv.org.tr)