AMNESTY INTERNATIONAL

28 February 2022 IOR 40/5276/2022

THE PRACTICAL APPLICATION OF THE GUIDING PRINCIPLES ON BUSINESS AND HUMAN RIGHTS IN THE TECH SECTOR

AMNESTY INTERNATIONAL SUBMISSION TO THE OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS

Amnesty International's submission to the Office of the High Commissioner for Human Rights on the Practical Application of the Guiding Principles on Business and Human Rights in the Tech Sector focuses on the topics Addressing Human Rights Risks in Business Models and Human Rights Due Diligence and End-Use, though it makes points that are also relevant to the topics of Accountability and Remedy and The State's Duty to Protect, or Regulatory and Policy Responses. Following each case study are case-specific recommendations with an overarching recommendation at the end.

ADDRESSING HUMAN RIGHTS RISKS IN BUSINESS MODELS

In November 2019, Amnesty International published ground-breaking research demonstrating how the surveillance-based business model of Google and Facebook poses a systemic threat to human rights.[1]

Google and Facebook (now Meta) have helped to connect and provide crucial services to billions of people around the world. To participate meaningfully in today's economy and society, and realise their human rights, people rely on access to the internet – and the tools Google and Facebook offer.

Despite the value of online platforms in enabling human rights online, the services come at a serious human rights cost.[2] Google and Facebook make their services conditional upon ubiquitous surveillance of their users, from search preferences to location tracking, which provides them extensive powers to exploit individual vulnerabilities.[3] Such practices are only increasing in breadth and depth in parallel with the erosion of any meaningful alternatives. As with all systems of surveillance, this has disproportionate impacts on marginalised groups, and exacerbates existing structural inequalities.[4]

The dominance of the gatekeeper platforms means people have become reliant on their services to facilitate the enjoyment of rights such as freedom of expression and the rights of peaceful assembly and association.[5] The companies' surveillance-based business model has created a paradoxical situation where for people to exercise their rights in the digital age, they are forced to accede to a business model that inherently undermines their human rights. Firstly, an assault on the right to privacy on an unprecedented scale, and then a series of knock-on effects that pose a serious risk to a range of other rights, from freedom of expression and opinion to freedom of thought and the right to equality and non-discrimination.

[1] Amnesty International, *Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights* (*Surveillance Giants*), 2019, https://www.amnesty.org/en/documents/pol30/1404/2019/en/.

[2] *Surveillance Giants*, 2019

[3] *Surveillance Giants,* 2019.

[4] See for example Pratyusha Kalluri, co-creator of the Radical AI Network, *Don't ask if artificial intelligence is good or fair, ask how it shifts power*, in Nature, July 2020, https://www.nature.com/articles/d41586-020-02003-2; Ruha Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code*, 2019.

[5] "In the digital age, the exercise of the rights of peaceful assembly and association has become largely dependent on business enterprises, whose legal obligations, policies, technical standards, financial models and algorithms can affect these freedoms." Special Rapporteur on the rights to freedom of peaceful assembly and of association, *Report on the rights to freedom of peaceful assembly and of association: The Digital Age*, 2019, (A/HRC/41/41)

Google and Facebook make most of their revenue through digital advertising (80 and 98% respectively), based on the accumulation and analysis of people's personal data. To increase their revenue from advertisers, they compete to offer the best predictions about the most people, which incentivises them to seek more data on more people. At the same time, the surveillance-based business model has in-built tendencies to exponentially increase the platforms' dominance and scale, and thus, the abuse of privacy and other rights has also helped concentrate power towards Google and Facebook. The extraction of ever more data has enabled the companies to gain greater control over the main ways that people engage with the internet, to an extent that likely would not have been possible had the companies stuck to a more privacy-respecting model.

The surveillance-based business model goes hand-in-hand with algorithmic recommender systems, aimed at keeping people's attention fixed on their screens for as long as possible so that they can be shown more ads and thus generate more revenue. These algorithms feed on people's personal data and online behaviour over time, profiling and manipulating them by presenting people content thought to be the most "relevant", while ensuring the greatest engagement to maximise revenues.[6] These algorithmic recommender systems tend to promote divisive and extreme content that is more likely to attract users' attention and keep them engaged, fuelling online misinformation and disinformation, the proliferation of online abuse and incitement to violence and racial discrimination.[7]

Recent revelations and research have further illustrated the harms of this surveillance-based business model. As evidenced by internal Facebook research, brought to the public's attention by whistle-blower Frances Haugen, a tweak in their algorithm has made angry voices louder and led to misinformation, toxicity and violent content being inordinately prevalent among reshares.[8] According to Facebook's own research, Instagram, has been shown to be harmful for teenage girls' mental health due to its addictive design and focus on social comparison and body image.[9] Despite these findings, Facebook has consistently downplayed Instagram's negative impacts on teenagers and has not made its research public or available to academics or lawmakers who have requested it. Most importantly, Facebook has taken little action to address these negative impacts.

Other studies have shown Facebook's ad delivery algorithms to be discriminatory, for instance excluding women and older people from seeing job ads.[10] These same algorithms have also been found to exploit mental vulnerabilities, such as pushing anxiety-fuelling ads at a young mother worrying about her toddler's health.[11]

There is also evidence that Facebook only acts where political pressure is the greatest and where it is most profitable for it to act, leaving millions of users in the Global South unprotected[12] and exposed to harmful, extreme and hateful content. This has often led to real-world hate and violence, such as in Myanmar and Ethiopia where Facebook failed to curb the spread of posts inciting violence against ethnic minorities.[13]

---

[6] European Data Protection Supervisor, *Opinion 1/2021 on the Proposal for a Digital Services Act*, 10 February 2021; European Data Protection Supervisor, *Opinion 3/2018 EDPS Opinion on online manipulation and personal data*, 19 March 2018.

[7] Amnesty International, *Silenced and misinformed: Freedom of expression in danger during Covid-19,* October 2021, p 27 www.amnesty.org/en/documents/pol30/4751/2021/en/; *Surveillance Giants,* 2019, p. 34

[8] Wall Street Journal, *Facebook Tried to Make Its Platform a Healthier Place. It Got Angrier Instead.,* September 15, 2021, https://www.wsj.com/articles/facebook-algorithm-change-zuckerberg-11631654215

[9] Wall Street Journal, *Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show*, September 14, 2021, https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739

[10] Global Witness, *How Facebook's ad targeting may be in breach of UK equality and data protection laws*, September 9, 2021, https://www.globalwitness.org/en/campaigns/digital-threats/how-facebooks-ad-targeting-may-be-in-breach-of-uk-equality-and-data-protection-laws/; Muhammad Ali, Piotr Sapiezynski, Miranda Bogen, Aleksandra Korolova, Alan Mislove, Aaron Rieke, *Discrimination through optimization: How Facebook's ad delivery can lead to skewed outcomes*, Proceedings of the ACM on Human-Computer Interaction 2019*, 2019,* https://arxiv.org/abs/1904.02095

[11] Panoptykon Foundation, *Algorithms of trauma: new case study shows that Facebook doesn't give users real control over disturbing surveillance ads,* September 28, 2021, https://en.panoptykon.org/algorithms-of-trauma

[12] Rest of World, *The Facebook Papers reveal staggering failures in the Global South*, October 28, 2021, https://restofworld.org/2021/facebook-papers-reveal-staggering-failures-in-global-south/

[13] The Guardian, *Rohingya sue Facebook for £150bn over Myanmar genocide*, December 6, 2021,

Amnesty International urges governments to:

- Ban surveillance advertising that relies on invasive tracking and the processing of personal data, and transition to non-invasive targeting tools such as contextual advertising.
- Ensure independent oversight over the algorithmic recommender systems used by online platforms and require them to be opt-in instead of an opt-out, to limit the amplification and spread of hate speech, disinformation, and other harmful content.
- Ensure people can practically choose rights-respecting alternatives to the dominant tech platforms, including by requiring interoperability so that people can freely move between these services and competing platforms.[14]

HUMAN RIGHTS DUE DILIGENCE AND END-USE

The United Nations Guiding Principles on Business and Human Rights (UN Guiding Principles) are clear that human rights due diligence encompasses the entire value chain, both upstream and downstream. The act of selling a product to a particular party in a particular jurisdiction or operating context may give rise to human rights risks that would need to be properly identified, analysed and addressed for the company to meet its corporate responsibility to respect human rights. Companies cannot ignore or discount adverse impacts that might be said to have been caused by another party, such as when an end-user of a product has misused a product in a way that causes human rights harms. However, research by Amnesty International shows that some companies in the tech sector are doing just that.

DIGITAL SURVEILLANCE TECHNOLOGIES

In 2020, Amnesty International published research showing that three companies based in the European Union (EU) sold digital surveillance technologies, such as facial recognition technology and network cameras, to the Chinese government, and that some of these sales were to end-users in the north-western region of Xinjiang.[15] In some cases, the export was directly for use in China's indiscriminate mass surveillance programmes, with the risk of being used against Uyghurs and other predominantly Muslim ethnic groups throughout the country. This investigation revealed that none of the companies conducted adequate human rights due diligence on the investigated transactions. In 2021, subsequent Amnesty International research showed that digital surveillance technologies, just like those being sold by the EU companies, are being used by Chinese government actors in Xinjiang during the commission of grave human rights violations against Uyghur and Muslim ethnic minorities.[16]

The companies should have known that sales to China's authorities were of significant risk, but they apparently took no steps to prevent their products from being used by human rights abusers nor could they provide Amnesty International with clear answers as to what due diligence they carried out before completing these sales. In responses to Amnesty International, some of these companies reported that they often have no knowledge of how their products will be used, and that even if they record intended uses and destinations pre-sale, they have no way of verifying what customers self-report after the sale.[17]

All businesses have a responsibility to conduct human rights due diligence, but it can be far more challenging for businesses who are deep within the technology stack. For example, Original Equipment Manufacturers (OEMs) who provide component parts for the products of another company, are most likely unable to track themselves what happens to their product after

---

https://www.theguardian.com/technology/2021/dec/06/rohingya-sue-facebook-myanmar-genocide-us-uk-legal-action-social-media-violence; CNN, *Facebook knew it was being used to incite violence in Ethiopia. It did little to stop the spread, documents show*, October 25, 2021, https://edition.cnn.com/2021/10/25/business/ethiopia-violence-facebook-papers-cmd-intl/index.html

[14] Amnesty International, *Interoperability as a tool to challenge platform power and protect human rights,* April 14, 2021, https://interoperability.news/2021/04/interoperability-as-a-tool-to-challenge-platform-power-and-protect-human-rights/

[15] Amnesty International, *Out of Control: Failing EU Laws for Digital Surveillance Export* (*Out of Control)*, (Index: EUR 01/2556/2020), September 21, 2020, https://www.amnesty.org/en/documents/eur01/2556/2020/en/

[16] Amnesty International, *"Like We Were Enemies in a War": China's Mass Internment, Torture, and Persecution of Muslims in Xinjiang*, (Index: ASA 17/4137/2021), June 10, 2021, https://www.amnesty.org/en/documents/asa17/4137/2021/en/

[17] *Out of Control*, p.28

it has been packaged and sold under a different brand name. Furthermore, many of these companies are small or medium enterprises who are at a disadvantage in negotiations with their larger customers and may not have any leverage to require adherence to human rights reporting requirements. This is a relatively common sales and distribution model in the surveillance technology industry, which implies that a significant part of the industry is currently not conducting any adequate or effective end-use human rights due diligence. This shows the need to create greater transparency through mandatory human rights due diligence, which "levels the playing field" and ensures greater cooperation between smaller and larger companies.

Amnesty International urges governments to:

- Ban the use, development, production, sale and export of facial recognition technology for identification purposes by both state agencies and private-sector actors.

UNLAWFUL TARGETED SURVEILLANCE

For years Amnesty International has warned of the human rights dangers posed by unlawful targeted surveillance generally and, in particular the international surveillance industry and vendor NSO Group. The Pegasus Project, a collaborative investigation coordinated by Forbidden Stories with the technical support of Amnesty International in July 2021 revealed how states' use of the targeted digital surveillance tools supplied by NSO Group, one of the industry's most prominent participants, is utterly out of control, destabilizing, and threatening to individuals' human rights.[18]

With the technical support of Amnesty International's Security Lab, the Pegasus Project revealed through forensic analysis, the targeting and infections of numerous devices of human rights defenders, journalists, lawyers, activists and politicians, including Heads of State, across the globe. In the months since the Pegasus Project revelations were first published there has been a steady stream of new damning evidence of digital attacks using Pegasus spyware, as well as a multitude of national, regional and international responses such as legal cases, investigations and statements from duty bearers.[19]

Despite the ground-breaking revelations and the increased attention on these issues, holding surveillance companies whose operations are shrouded in secrecy to account remains difficult. Very often, they hide behind arguments of 'security considerations' or 'confidentiality clauses' to keep information on their activities out of the public domain. Little is known about these companies or their corporate structures. Many do not disclose data on export licenses or contracts and have either no provisions for conducting human rights due diligence and remedy for abuses or have entirely unsatisfactory ones.[20] This, coupled with a lack of regulatory oversight and weak export licensing frameworks at domestic, regional and international levels, has made the task of regulating this industry extremely challenging.

NSO Group itself has acknowledged that its spyware tools may serve unlawful ends and contribute to adverse human rights impacts.[21] Despite this, the company has repeatedly failed to demonstrate how its human rights due diligence policies and practices are fit for purpose. This lack of action is seemingly driven by overriding national security considerations.[22]

---

[18] Amnesty International, *Uncovering the Iceberg: The Digital Surveillance Crisis Wrought by States and the Private Sector (Uncovering the Iceberg)*, 2021, https://www.amnesty.org/en/wp-content/uploads/2021/07/DOC1044912021ENGLISH.pdf

[19] The Guardian, *The Pegasus Project*, https://www.theguardian.com/news/series/pegasus-project

[20] Amnesty International, *Ending the Targeted Digital Surveillance of Those Defending Our Rights: A Summary of the Impact of the Digital Surveillance Industry on Human Rights* (Index: ACT 30/1385/2019), 2019, https://www.amnesty.org/en/documents/act30/1385/2019/en/

[21] NSO Group, Transparency and Responsibility Report 2021, 30 June 2021, nsogroup.com/wpcontent/uploads/2021/06/ReportBooklet.pdf, pp. 9; 17-19.

[22] See, e.g., NSO Group, Transparency and Responsibility Report 2021, 30 June 2021, nsogroup.com/wpcontent/uploads/2021/06/ReportBooklet.pdf, pp. 9-10 ("Our customers are solely authorized intelligence and law enforcement agencies responsible for investigating and, where possible, preventing serious crimes and terrorist acts. To effectively conduct these types of operations, these agencies must operate discreetly in order to (i) infiltrate criminal and terrorist networks to obtain information critical to stopping illegal acts, and (ii) avoid inadvertently giving criminals and terrorists a chance to thwart preventive activities. As a result, our customers mandate strict confidentiality from us and all other service providers in our sector. Our capacity for action is also limited by the fact that we do not have visibility into the specific operational uses of our products, unless that access is granted by the customer (as contractually required in the event of an investigation of suspicion that the system has been misused). Nonetheless, this report provides insights into how we operationalize our mission, and contribute to balance the tensions between the duties of states to protect their populations from physical and criminal threats with their

The mere assertion of national security, without the required demonstration of legality, necessity, proportionality or legitimate aim, has sufficed to justify the continued supply and operation of NSO Group's spyware tools. Neither the company nor state export authorities have been transparent about who the end-user clients of these technologies are and how they fulfil the requirements of company due diligence, mitigation mechanisms, or export licence decisions. Due to secrecy and confidentiality requirements, it is questionable whether an industry dependent on governments – including those who routinely clamp down on human rights – as its customer base can or will ever provide the appropriate disclosures to enable adequate scrutiny.

The case of NSO Group demonstrates that even companies that know or should have known of abuses continue to supply their surveillance technology and face few consequences. NSO Group claims to have no insight into the targets selected by clients. But this is no answer. The failure to take note of the easily knowable risks of selling surveillance tools to the clients reveals a shocking failure to carry out due diligence on the company's part. A company cannot avoid responsibility through such "wilful blindness" to risks of their sales and products and as a reasonable person would appreciate; even if NSO Group had no knowledge of the specific abuses linked to its product, in these circumstances, it ought reasonably to have known that abuse would occur.[23] Surveillance companies like NSO Group appear to have embraced complicity in pursuit of greater revenues.

CORPORATE COMPLICITY UNDER INTERNATIONAL LAW AND STANDARDS[24]

Complicity – as a legal concept – takes several forms, from individual criminal or civil liability as defined in domestic legal systems, to international criminal law involving corporate involvement in international crimes.

In this submission, Amnesty International uses the term "complicity" to be understood according to evolving norms of international law and standards applicable to private companies – or "legal persons", as they may be described in domestic legal systems.

The principle has evolved and is reflected in several leading international standards, variously applicable to international crimes, and other human rights harms. The commentary on the UN Global Compact makes clear that complicity in this context contains two primary elements:

- "An act or omission (failure to act) by a company, or individual representing a company, that "helps" (facilitates, legitimizes, assists, encourages, etc.) another, in some way, to carry out a human rights abuse, and
- The knowledge by the company that its act or omission could provide such help."[25]

---

obligations towards freedom of expression, the right to privacy and other human rights.").

[23] As explained in the Guidance to the United Nations' Ten Principles of the UN Global Compact, complicity for corporations means "being implicated" in human rights abuses. It is "generally" made up of two elements: an act by a company or its representative that "helps" another "in some way, to carry out a human rights abuse" and the "knowledge by the company that its act or omission could provide such help". This formulation requires only that the corporate act facilitate human rights abuses but does not mandate that the aid be substantial or a "but for" cause of the abuse. It also finds complicity based on knowledge that the aid could facilitate human rights abuse, without any requirement that the corporation know that it will in fact facilitate these abuses. United Nations Global Compact, "Principle Two: Human Rights", The Ten Principles of the UN Global Compact, unglobalcompact.org/what-is-gc/mission/principles/principle-2.

Corporations cannot escape complicity by wilful blindness. Instead, corporate knowledge can be deduced based on evidence of what was generally known, and thus what a reasonable corporation should know and likely in fact does know. The inquiry is comparable to that used to determine corporate negligence: one asks whether "a reasonable person in the company's shoes, with the information reasonably available at the time, would have known that there was a risk that its action would harm a person. This means that [one] will look at both what the company itself knew, and what a reasonable company in its shoes would have known about the risk that harm would occur." Publicly available information, as well as information brought to the attention of the company, is relevant in determining a company's knowledge. The company need not know the "full extent of the gross human rights abuses to which it contributes, provided some of the abuses are known." International Commission of Jurists (ICJ), Report of the ICJ Expert Legal Panel on Corporate Complicity in International Crimes, 1 January 2008, icj.org/report-of-the-international-commission-of-jurists-expert-legal-panel-on-corporate-complicity-in-internationalcrimes, at 20-22.

[24] *Uncovering the Iceberg*

[25] United Nations Global Compact, "Principle Two: Human Rights", *The Ten Principles of the UN Global Compact*, unglobalcompact.org/what-is-gc/mission/principles/principle-2.

It continues, for the avoidance of doubt: "[s]hould a corporation benefit from violations by the authorities, or entice, encourage or support them in violating human rights, corporate complicity would be evident."[26]

NSO Group's sales and products have enabled widespread violations, and evidence of this risk was readily available, whether they chose to take note of it or not. International human rights standards are designed to prevent the outsourcing of human rights responsibilities specifically in situations where the lines of the state/corporate nexus become blurred. Indeed, even confronted with these shocking disclosures, it is still uncertain whether states will hold each other to account, or whether NSO Group will ultimately face real consequences.

Whether or not the evident complicity of NSO Group in state human rights violations amounts to grounds for civil or criminal liability under domestic, regional or international systems is a question to be answered by states, who owe an obligation of remedy to the victims of violations revealed in the Pegasus Project.

Rather alarmingly, in the face of various disclosures by civil society, the trend in the surveillance industry at present is toward reduced – not enhanced – transparency. Technical developments in spyware operation, such as incorporation of zero-click infection and network injection, are pushing awareness of and visibility into targeted attacks further out of reach. At the same time, private investment in the surveillance industry, through private equity or other private funds, compound the lack of independent oversight.

While NSO Group released a first Transparency and Responsibility Report in June 2021, the report merely serves to illustrate the limits of the surveillance industry's tolerance of transparency. Transparency is a key aspect of the corporate responsibility to respect human rights, as articulated by the UN Guiding Principles, yet the industry is failing to engage in meaningful transparency efforts.

These revelations show the urgent need for meaningful control over the rampant abuses being carried out. These disclosures make clear that when states fail to respect human rights through surveillance or fail in their duties to protect us against human rights abuses by companies at home or abroad, these same companies will be able to continue flouting their human rights responsibilities with impunity.

Amnesty International urges governments to:

- Impose an immediate moratorium on the sale, transfer, and use of spyware technology. There is an urgent need to halt activities of states and companies, until there is a robust human rights regulatory framework in place
- Conduct immediate, independent, transparent and impartial investigations into all export licences granted for spyware technology and revoke all marketing and export licences in situations where there is a substantial risk such technology could contribute to human rights violations.

GENERAL RECOMMENDATION:

The UN Guiding Principles make clear that states must protect against human rights abuse within their territory and/or jurisdiction by third parties, including business enterprises. This requires taking appropriate steps to prevent, investigate, punish and redress such abuse through effective policies, legislation, regulations and adjudication. States must put in place legislation that addresses the harms arising from companies' failure to conduct adequate due diligence, including on the end-use and end-users of their products. Therefore, Amnesty International is calling on governments to:

- Ensure that all companies domiciled in their territories are required to act responsibly and are held liable for their negative human rights impacts. States must require by law that these companies conduct human rights due diligence on their global operations, supply chains and in relation to the use of their products and services. Companies should be compelled to identify, prevent, mitigate and account for how they address the human rights-related risks of their activities and business relationships. This should include liability for harm caused and access to remedy in the home states of the companies, for affected communities.

[26] Andrew Clapham, "On Complicity" in M. Henzelin and R. Roth (editors), *Le droit penal a l'epreuve de l'internationalisation*, 2002, ssrn.com/abstract=1392988, pp. 241-275.