## Identified gap in the OECD Guidelines: digitalisation and digital technology

**Outcome sought:** Broad and comprehensive stocktaking of the OECD Guidelines for Multinational Enterprises (Guidelines) that addresses gaps on digitalisation and digital technology.

**Problem: The OECD Guidelines do not acknowledge the increasing digitalisation of the global economy, nor set standards for business on avoiding adverse human rights and environmental impacts linked to digitalisation**

The digitalisation of the global economy is altering and often exacerbating the potential for all MNEs (not merely technology companies) to adversely impact human rights and the environment. Digital technologies may have positive impacts on human rights (such as enhancing freedom of expression and the right to information), but can also facilitate violations of the rights to non-discrimination, privacy, freedom of speech/political participation, life, liberty, security, and economic, social and cultural rights, among others. Digitalisation is therefore linked to numerous challenges for responsible business conduct (RBC). The following issues are of particular concern to civil society:

- The need for all MNEs operating in the digital economy – not just well-known, global tech companies – to recognise the potential harms they may be connected to as a result of the digitalisation of their activities, and the need for them to conduct human rights due diligence over those impacts;
- New types of entities such as social media and online service providers/platforms have changed the concept of the 'MNE', raising the problems of inadequate taxation of and stakeholder consultation by non-brick-and-mortar MNEs, and securing accountability for the harmful impacts of MNEs not clearly tied to any specific country and legal jurisdiction;
- The commercialisation of big data, as well as the growth of digital technologies such as AI, surveillance/telecommunications technologies, and online/social media platforms, have enabled violations of numerous human rights (affecting both average citizens and human rights defenders in particular). Biases built into the massive datasets used to train automated systems and large language models can result inprivacy violations and discrimination at scale,[1] with systems 'learning' to discriminate along the lines of race, gender and income.[2] This disproportionately harms already at-risk and vulnerable groups, such as women, non-binary persons, racial and ethnic minorities, migrants and religious minorities, among others. Users of platforms can also use them to engage in discrimination that should be better addressed by platform owners. Further, 'profiling' of individuals based on their online activities may facilitate discrimination and privacy violations.[3] These technologies have also increased capacity for facilitation of violence, manipulation of democratic values, rapid spread of mis- and disinformation, and human rights abuses by governments or average users;
- The need for MNEs to conduct human rights due diligence during the design/development stage of a technology rather than (as is common) immediately prior to its deployment, as well as conduct auditing of systems for algorithmic bias and subsequently mitigate issues found before the model is deployed;
- Many digital technologies are subject to "dual-use" authorisation and licensing, and while some dual-use processes take into account human rights, they are not necessarily aligned with the due diligence expectations of the OECD Guidelines;
- The sheer scale and market share across diverse types of goods held by certain platform MNEs, particularly surveillance capitalists, raise serious concerns about consumer wellbeing as well as competition and suppression of information and innovation;

- Telecommunications companies' responsibility to enable access to technology and advance digital inclusion globally, on one hand, and to refrain from shutting down networks ('internet shutdowns') or transferring user data to governments, on the other hand;
- The environmental (from minerals mining to the massive and growing climate impact of data centres[4]), labour rights, and human rights impacts caused through the supply chains of technology hardware MNEs are too often overlooked. This problem is exacerbated by the extreme lack of transparency in the sector,[5] particularly regarding MNEs' business relationships with (authoritarian) governments.[6]
- Increased digitalisation (and automation) in many industries has disrupted workplaces, causing serious and gendered impacts to the rights and wellbeing of workers. Low paid female workers are at much higher risk of bearing the brunt of displacement by automation compared to male workers.[7] Women and girls are also less likely to benefit from digitalisation,[8] evidence of a 'digital gender divide' which has been further exacerbated by the fallout from the COVID-19 pandemic.[9]

Despite the myriad adverse impacts of MNEs in the context of digitalisation, the OECD Guidelines do not adequately establish standards in this sphere. Chapter II (General Policies) minimally "encourages" enterprises to "promote Internet Freedom through respect of freedom of expression, assembly and association online." Additionally, Chapter IX (Science and Technology) focuses narrowly on protection of intellectual property, sharing of technological and scientific knowledge with host countries, and coordination of business activities with national science agendas and universities. The chapter says nothing about ways in which digitalisation can impact MNEs' potential to cause, contribute to, or be directly linked to adverse impacts, nor does it address the importance for MNEs of conducting supply chain due diligence over their digitalisation-related impacts. Critically, other chapters such as Disclosure (III), Human Rights (IV), Employment and Industrial Relations (V), Environment (VI), Consumer Protection (VIII) and Taxation (XI) do not include language reflecting the nexus between the issue covered in that chapter and RBC expectations for MNEs in the context of digitalisation.

**Impact of the problem: Lack of clear standards for MNEs on RBC in the context of digitalisation and limited access to remedy for impacted parties.**

The lack of expectations in the Guidelines for MNEs to act responsibly in the context of digitalisation has two primary consequences:

1) Lack of understanding by MNEs on expectations for them to prevent and mitigate the adverse effects of digitalisation; and
2) Diminished grounds on which to seek remedy via the National Contact Point (NCP) grievance mechanisms.
    a. A handful of specific instances have sought remedy for harmful impacts linked to digitalisation.[10] These complaints have addressed issues such as the sale of surveillance/telecommunications technologies to repressive governments (and the subsequent misuse of those technologies)[11] and the failure of online marketplaces to prohibit third-party sales of goods used for illegal and environmentally harmful purposes.[12] NCPs have reached widely divergent outcomes, even when addressing the same exact issue.[13] Further, NCPs have rejected complaints by erroneously concluding that dual-use authorisation for surveillance/telecommunications technologies is sufficient for human rights due diligence, although this is not the case.[14] The increasing number of specific instances on technological matters, along with the spotty acceptance and agreement rates at NCPs, demonstrate a need for

clearer expectations to both guide MNEs' conduct and help NCPs apply the Guidelines in complaints.

**Parallel laws and standards**

Analysis of gaps in the OECD Guidelines on digitalisation could draw on the following standards, initiatives, and guidelines:

- International standards and covenants including the OHCHR's B-Tech Project,[15] the UN's Internet Governance Forum,[16] the UN Secretary General's Roadmap for Digital Cooperation,[17] the UN Strategy and Plan of Action on Hate Speech,[18] UNESCO's ROAM principles,[19] the WTO's Declaration on Global Electronic Commerce,[20] the ILO's Agenda for the Future of Work,[21] and APEC's Roadmap on Internet and Digital Economy;[22]
- The OECD due diligence guidance as well as the OECD Privacy Guidelines,[23] the Cancun Declaration,[24] and various OECD Recommendations such as those on Health Data Governance, Digital Security, Risk Management for Economic and Social Prosperity, Digital Security of Critical Activities, AI, Internet Policy Making, Facilitating International Technology Co-operation Involving Enterprises, Consumer Protection in E-commerce, and ICT and the Environment;
- Regional legislation and regulations such as the EU's General Data Protection Regulation (GDPR),[25] the Regulation on the free flow of non-personal data,[26] the Cybersecurity Act,[27] the Open Data Directive,[28] Ethics Guidelines for Trustworthy AI,[29] the EU Digital Services Act and the Digital Markets Act (currently under preparation),[30] and the Council of Europe's Convention 108+ for the protection of individuals with regard to the processing of personal data;[31]
- The European Commission's proposed initiative to align dual use technology authorisation with human rights due diligence standards;[32]
- National guidance and laws, such as Australia's Sharing of Abhorrent Violent Material Act 2019,[33] Chile's National AI Policy,[34] and numerous countries' legislation and recommendations on AI, digital platforms, and social media;
- Multi-stakeholder initiatives such as The Christchurch Call[35] championed by New Zealand and France, the Partnership on AI,[36] the Global Network Initiative,[37] and the Santa Clara Principles which call for transparency by social media companies;[38]
- Civil Society guidelines such as the Danish Institute for Human Rights' guidance on addressing digital technologies in National Action Plans on Business and Human Rights,[39] the Global Network initiative to develop a framework of principles and guidance for the ICT industry,[40] the Toronto Declaration,[41] and Ranking Digital Rights[42] which aim to trigger a 'race to the top' on digital rights;[43] and
- Industry standards, such as Google's 2018 AI principles.[44]

**Why ensuring a comprehensive stocktaking on gaps is important**

The OECD Guidelines, originally drafted in 1976, have not been revised since 2011 and are out of date in many ways. Ten years of implementation of the current text of the Guidelines have revealed numerous gaps in the text that cause both a serious lack of clarity and coherence in international norms on key elements of responsible business conduct, and diminish victims' chances for remedy and accountability via the NCPs. Meanwhile, recent developments in RBC standards made beyond the OECD Investment Committee are threatening to make the OECD Guidelines comparatively less useful or even obsolete. The OECD Investment Committee's Working Party on Responsible Business Conduct (WPRBC), responsible for the OECD Guidelines, has begun a stocktaking to identify what gaps exist in the Guidelines and assess whether steps are needed to address them. A comprehensive stocktaking that addresses all the gaps identified by civil society and other stakeholders is essential to evaluate whether the Guidelines are still fit for purpose.

**Who needs to act?**
OECD Watch urges governments to show commitment to keeping the OECD Guidelines up to date with evolving issues in the field of business and human rights – and acknowledge civil society's concerns regarding the current limitations in the Guidelines' standards and the NCP complaint system – by ensuring that the stocktaking studies all the issues of concern to civil society. OECD Watch also urges that states ensure the final stocktaking report responds to each concern raised by civil society. OECD Watch welcomes the stocktaking and stands ready to support the review process and any further steps taken to address gaps identified.

**About OECD Watch**
OECD Watch is a global network with over 130 member organisations in more than 50 countries. Founded in 2003, OECD Watch's primary aim is to help support CSO activities related to the OECD Guidelines and the work of the OECD's Investment Committee. Membership consists of a diverse range of civil society organisations – from human rights to environmental and development organisations, from grassroots groups to large, international NGOs – bound together by their commitment to ensuring that business activity contributes to sustainable development and poverty eradication, and that corporations are held accountable for their adverse impacts around the globe. For more information, please visit www.oecdwatch.org.

| | |
|---|---|
| **OECD Watch Secretariat** (c/o SOMO)<br>Sarphatistraat 30<br>1018 GL Amsterdam<br>The Netherlands<br>Ph: +31 20 6391291<br>info@oecdwatch.org, www.oecdwatch.org | Marian Ingrams, Esq., Coordinator & Researcher, m.ingrams@oecdwatch.org<br><br>Dr. Joseph Wilde-Ramsing, Senior Researcher and Coordinator, j.wilde@oecdwatch.org |

[1] Karen Hao, "We read the paper that forced Timnit Gebru out of Google. Here's what it says", MIT Technology Review 4 December 2020, available at: https://www.technologyreview.com/2020/12/04/1013294/google-ai-ethics-research-paper-forced-out-timnit-gebru/. The Cambridge Analytica scandal is perhaps the most well-known example of individuals' data being harvested and used to build (voter) psychological profiles. See N. Confessore, "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far," The New York Times, 4 April 2018, available at: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.
[2] For more information see Karen Hao, "This is how AI bias really happens—and why it's so hard to fix", MIT Technology Review, 4 February 2019, available at: https://www.technologyreview.com/2019/02/04/137602/this-is-how-ai-bias-really-happensand-why-its-so-hard-to-fix/.
[3] The Cambridge Analytica scandal is perhaps the most well-known example of individuals' data being harvested and used to build (voter) psychological profiles. See N. Confessore, "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far," The New York Times, 4 April 2018, https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.
[4] Emma Strubell, Ananya Ganesh and Andrew McCallum, "Energy and Policy Considerations for Deep Learning in NLP", University of Massachusetts Amherst, 5 June 2019, available at: https://arxiv.org/abs/1906.02243.
[5] The need to protect 'trade secrets' are used as a shield from scrutiny, see Mind the Gap, 'CASE STUDY: Samsung's nondisclosure of chemical usage', 2020, available at: https://www.mindthegap.ngo/harmful-strategies/constructing-deniability/refusing-to-disclose-information/example-samsungs-nondisclosure-of-chemical-usage/.
[6] See Mind the Gap, 'Aligning with suppressive State institutions', 2020, available at: https://www.mindthegap.ngo/harmful-strategies/utilising-state-power/aligning-with-suppressive-state-institutions/.

[7] See Mariya Brussevich, Era Dabla-Norris, Salma Khalid, 'Is Technology Widening the Gender Gap? Automation and the Future of Female Employment', May 6, 2019, available at: https://www.imf.org/en/Publications/WP/Issues/2019/05/06/Is-Technology-Widening-the-Gender-Gap-Automation-and-the-Future-of-Female-Employment-46684; The impacts of rapid automation are already being seen in the Bangladesh apparel industry where female workers' participation has declined: The Daily Star, 'Women garment workers on the decline', December 15, 2020, available at: https://www.thedailystar.net/business/news/women-garment-workers-the-decline-2011601.
[8] See OECD (2018), 'Bridging the Digital Gender Divide: Include, Upskill, Innovate', available at: http://www.oecd.org/digital/bridging-the-digital-gender-divide.pdf.
[9] Valentina Romei, 'Pandemic boost to tech and digital industries worsens gender job divide', Financial Times, 22 November 2020, available at: https://www.ft.com/content/21ae50e1-56e6-43d4-acc2-d6fc45dba447.
[10] The Grupa OLX and AirBnB cases, available at: https://mneguidelines.oecd.org/Digitalisation-and-responsible-business-conduct.pdf.
[11] *See, e.g., Privacy Int'l et al. vs. Gamma International*, available at: https://complaints.oecdwatch.org/cases/Case_286.
[12] *See Frank Bold vs. Grupa OLX sp. z o.o.*, available at: https://complaints.oecdwatch.org/cases/Case_523.
[13] Compare the British NCP's consideration of the human rights impacts of company Trovicor's sale of surveillance technology to Bahrain in *Privacy Int'l et al. vs. Trovicor,* available at: https://complaints.oecdwatch.org/cases/Case_287, with the German NCP's rejection of the same claims against Gamma International in *Privacy Int'l et al. vs. Gamma International*, available at https://complaints.oecdwatch.org/cases/Case_286.
[14] *See, e.g.*, *FIDH, JFI and Redress vs. Italtel*, available at: https://complaints.oecdwatch.org/cases/Case_496.
[15] OHCHR, B-Tech Project, available at: https://www.ohchr.org/EN/Issues/Business/Pages/B-TechProject.aspx.
[16] Internet Governance Forum, available at: https://www.intgovforum.org/multilingual/.
[17] United Nations General Assembly, Road map for digital cooperation: Implementation of the recommendations of the High-level Panel on Digital Cooperation, 29 May 2020, A/74/821, available at: https://undocs.org/A/74/821.
[18] United Nations, United Nations Strategy and Plan of Action on Hate Speech, September 2020, available at: https://www.un.org/en/genocideprevention/documents/UN%20Strategy%20and%20PoA%20on%20Hate%20Speech_Guidance%20on%20Addressing%20in%20field.pdf.
[19] UNESCO ROAM-X Indicators, available at: https://en.unesco.org/internet-universality-indicators/roamx-indicators
[20] WTO *Work Programme on Electronic Commerce,* WT/L/274 (30 September 1998).
[21] ILO Centenary Declaration for the Future of Work (2019), available at: https://www.ilo.org/wcmsp5/groups/public/---ed_norm/---relconf/documents/meetingdocument/wcms_711674.pdf.
[22] APEC Roadmap on Internet and Digital Economy, 2017, 2017/CSOM/006.
[23] OECD (2013), The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at: http://www.oecd.org/digital/ieconomy/privacy-guidelines.htm.
[24] OECD (2016), Ministerial Declaration on the Digital Economy (Cancún Declaration) available at: http://www.oecd.org/digital/Digital-Economy-Ministerial-Declaration-2016.pdf.
[25] European Parliament, The General Data Protection Regulation, Regulation 2016/679, available at: http://data.europa.eu/eli/reg/2016/679/2016-05-04.
[26] European Parliament, The Regulation on the free flow of non-personal data, Regulation 2018/1807, available at: http://data.europa.eu/eli/reg/2018/1807/oj.
[27] European Parliament, The EU Cybersecurity Act, Regulation 2019/881, available at: https://eur-lex.europa.eu/eli/reg/2019/881/oj.
[28] European Parliament, Open Data Directive, Directive 2019/1024, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.172.01.0056.01.ENG.
[29] European Commission, (2018), Ethics Guidelines for Thrustworthy AI, available at: https://ec.europa.eu/futurium/en/ai-alliance-consultation.
[30] European Commission, "The Digital Markets Act: ensuring fair and open digital markets", available at: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.
[31] Council of Europe, Convention 108 +: Convention for the protection of individuals with regard to the processing of personal data, June 2018, available at: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.
[32] European Commission, "Commission welcomes agreement on the modernization of EU export controls," 9 November 2020, https://trade.ec.europa.eu/doclib/press/index.cfm?id=2209.
[33] Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019, available at: https://www.legislation.gov.au/Details/C2019A00038.
[34] The Chilean Artificial Intelligence Policy (2019), available at: https://oecd.ai/dashboards/policy-initiatives/2019-data-policyInitiatives-24840
[35] The Christchurch Call, (2019), available at: https://www.christchurchcall.com/.
[36] Partnership on AI, (2016), available at: https://www.partnershiponai.org/.

[37] Global Network Initiative, available at: https://globalnetworkinitiative.org/.
[38] The Santa Clara Principles on Transparency and Accountability in Content Moderation. (2018), Available at: https://santaclaraprinciples.org/.
[39] The Danish Institute for Human Rights, (2020), Human rights impact assessment of digital activities, available at: https://www.humanrights.dk/publications/human-rights-impact-assessment-digital-activities.
[40] Global Network Initiative, (2018), The GNI Principles, available at: https://globalnetworkinitiative.org/gni-principles/.
[41] Amnesty International, (2018) The Toronto Declaration, available at: https://www.torontodeclaration.org/.
[42] Ranking Digital Rights, https://rankingdigitalrights.org/.
[43] OECD (2020), Digitalisation and RBC: Stocktaking of policies and initiatives, https://mneguidelines.oecd.org/Digitalisation-and-responsible-business-conduct.pdf.
[44] Google, (2018), Artificial Intelligence at Google: Our Principles, available at: https://ai.google/principles/.