THE GLOBAL DIGITAL COMPACT AND INTERNATIONAL LAW

MAY 2023

Workshop summary report

MINDEROO CENTRE FOR TECHNOLOGY & DEMOCRACY

May 2023

Minderoo Centre for Technology and Democracy and the Lauterpacht Centre for International Law

Minderoo Centre for Technology and Democracy

The Minderoo Centre for Technology and Democracy is an independent team of academic researchers at the University of Cambridge, who are radically rethinking the power relationships between digital technologies, society and our planet.

www.mctd.ac.uk

THE GLOBAL DIGITAL COMPACT AND INTERNATIONAL LAW

Workshop co-hosted by Prof Henning Grosse Ruse-Khan and Dr Ann Kristin Glenster

5-7pm 2 May 2023, Lauterpacht Centre for International law, University of Cambridge

Workshop summary report: Dr Ann Kristin Glenster, Senior Policy Advisor, Minderoo Centre for Technology and Democracy

On 2 May 2023, the Minderoo Centre of Technology and Democracy and the Lauterpacht Centre for International Law convened a workshop to discuss international law implications of the Minderoo Centre for Technology and Democracy's recently submitted evidence to the proposed Global Digital Compact (GDC).

The idea for a GDC was introduced in the United Nations Secretary General's report Common Agenda (2021),[1] with the intention that it would "outline shared principles for an open, free and secure digital future for all."[2] Input into the GDC was subsequently requested by the United Nations Office of the Secretary-General's

[1] Secretary-General, *Our Common Agenda – Report of the Secretary-General* (United Nations 2021) https://www.un.org/en/content/common-agenda-report/ accessed 04 May 2023.
[2] United Nations, Office of the Secretary-General's Envoy on Technology, https://www.un.org/techenvoy/global-digital-compact accessed 4 May 2023.

Envoy on Technology addressing "core principles that all governments, companies, civil society, and other stakeholders should adhere to" and "key commitments to bring about these specific principles" in relation to seven digital issues.[3] The evidence will be collated and presented at the United Nations Summit of the Future in September 2024.

Responding to the call for evidence, the Minderoo Centre for Technology and Democracy convened two sessions with academic researchers from the University of Cambridge in April 2023. Evidence from these sessions was submitted and collated into a report published by the Minderoo Centre for Technology and Democracy.[4] The evidence report addressed the seven digital issues identified in the call for submissions:

1. Connect all people to the Internet, including all schools
2. Avoid Internet fragmentation
3. Protect data
4. Apply human rights online
5. Introduce accountability criteria for discrimination and misleading content
6. Promote regulation of artificial intelligence
7. Digital commons as a global public good

This workshop specifically discussed whether the proposed core principles and key commitments should be amended, extended, or deleted, and the mechanisms that would be needed in international law to give them effect.

[3] https://www.un.org/techenvoy/global-digital-compact/submissions accessed 4 May 2023.
[4] Minderoo Centre for Technology and Democracy, Evidence Submitted to the Global Digital Compact (April 2023) https://www.mctd.ac.uk/evidence-submitted-to-the-global-digital-compact/ accessed 4 May 2023.

KEY TAKEAWAYS

Key takeaways from the workshop are:

- The principle of connecting all people to the Internet first concerns access, and second the rights and protections which should apply once people are connected to the Internet
- Principles of cybersecurity and safety are crucial, especially to safeguard critical infrastructure
- International law lacks effective mechanisms to compel private actors, especially key intermediaries, to adhere to human rights or other standards. While it can oblige States to act, those are often unwilling or unable to impose obligations on relevant private actors that uphold human rights or other shared values. Internet companies and social media platforms' internal policies and adjudication processes cannot be relied upon by individual users to guarantee their user rights, including the enforcement of human rights
- Accountability has to be more than mere transparency, and for this purpose, researchers, courts, and regulators must have access to data and systems as a matter of law. In addition, accountability must reflect the core role of private actors in implementing, interpreting and enforcing state rules in the digital context
- The digital commons as a global public good should be governed by international law frameworks, including the Rabat Plan of Action[5]

[5] Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence (https://www.ohchr.org/en/freedom-of-expression#:~:text=The%20Rabat%20Plan%20of%20Action%20suggests%20a%20high%20threshold%20for,article%2020%20of%20the%20ICCPR accessed 4 May 2023).

1. THE IMPORTANCE OF ACCESS

The workshop began by considering the first digital issue of connecting all people to the Internet. Workshop participants observed how this should be a core principle as it is a prerequisite for the other core principles. Hence, this digital issue could be conceptualised as having two steps: (1) Connect all people to the Internet as a right that should be provided by governments; and (2) The rights that should follow, such as being protected from online harms, once individuals are connected to the Internet. Applying this conceptualisation, the first step addresses issues such as net neutrality and States' obligations to provide necessary infrastructure to enable people to connect to the Internet. The second step concerning the online experience links to the issue of protecting human rights online and the difficulties of balancing freedom of speech with the right to participate and access to speech, which are placed in peril when people, especially women and girls, are driven offline or harassed into self-silence.[6] In that regard, workshop participants discussed how existing conceptualisations of human rights and user rights do not address the issue of amplification from harm arising from automation and cannot adequately address the essential role of platforms as private intermediaries.

2. CYBERSECURITY AND SAFETY

Workshop participants repeatedly noted the importance of cybersecurity in relation to a GDC. For instance, issues of cybersecurity were seen as crucial to delivering the ambition of connecting all people to the Internet as the infrastructure needed to do so must be safe and secure.

[6] The workshop participants specifically discussed the UK Online Safety Bill (https://bills.parliament.uk/bills/3137 accessed 4 May 2023) and the European Union Proposal for a Directive of the European Parliament and of the Council on combating violence against women and domestic violence (COM/2022/105 final) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0105 accessed 4 May 2023.

Workshop participants noted that this is especially the case where a commercial tech company provides Internet access to an entire country. India, Brazil, and Myanmar were cited as examples. In the cases of Brazil and Myanmar, it was noted how Meta had been used to spread political misinformation and disinformation, in at least one case with disastrous consequences.[7] Another example was concern over location and traffic data used by a Chinese taxi app as such data could be used deliberately to create traffic jams. Workshop participants also discussed the importance of cybersecurity to protect against cyberattacks from hostile foreign states.

Workshop participants identified issues of cybersecurity in relation to the ambition to avoid Internet fragmentation. The workshop specifically considered the the Minderoo Centre of Technology and Democracy evidence report's key commitment on open source software (OSS).[8] Workshop participants suggested that the key commitment listed in the evidence should be extended to include a commitment to ensure that OSS was safe and secure.[9] Workshop participants also discussed how the international community should create an international entity with the responsibility to identify and maintain critical OSS.

3. PROTECTING HUMAN RIGHTS AND USERS RIGHTS ONLINE

Some workshop participants felt that the Minderoo Centre for Technology and Democracy evidence report should have included more references to specific international human rights instruments.[10]

---

[7] e.g. the Bolsonaro's use of WhatsApp to spread political messages and the Rohnigya genocide in Myanmar.

[8] Digital Issue 2. Avoid Internet Fragmentation, core principle 1, key commitment 4: "All stakeholders should commit to ensuring the availability of repairable, free-and-open source software (FOSS) and sustainable devices". MCTD evidence report p. 7.

[9] *ibid.*

[10] For example, the Rabat Plan of Action (*supra* note 5).
There was a view that the wording of "necessary for a democratic society" taken from the European Convention of Human Rights should be replaced by the phrase 'international law and human rights' in digital issue 1, commitment 5 stating that "Access to the Internet should only be taken away by government in accordance with law necessary for democratic society" (MCTD evidence report, p. 5, original wording).

There was consensus among the workshop participants that challenges for international law in regard to human rights online concerned the issue of ensuring that individuals have effective remedies, particular in relation to human rights breaches across national borders, i.e., where the victim was in one country and the perpetrator in another.

Workshop participants discussed how the difficulties in international law were to find ways to compel States to impose positive human rights obligations on private actors, such as Internet companies and social media platforms, beyond soft law calls for social corporate responsibility (SCR).

Workshop participants expressed some lack of faith in depending on national laws and national courts to enforce online human rights, and workshop participants also noted anecdotally that representatives from social media platforms had referred to their own internal platform policies first to resolve issues, and national law second and only when an issue could not be satisfactorily addressed through internal policies. As a consequence, workshop participants noted how hard it is for individual users of Internet services, platforms, and products to seek redress through these policies when the access to the rights afforded in the policies were obfuscated by design. In practice, users must first go through the corporate architecture of internal policies before being able to invoke their legal rights. While users might at times enjoy the theoretical possibility to seek redress in front of national courts, the lack of effective availability of such remedies and the problems of enforcing any rulings (domestically, but even more so abroad) render these options inutile. It was clearly felt by workshop participants that relying on social media platforms and Internet companies' own adjudicative processes amounted to little more than a sham.[11]

[11] For example, there was some discussion regarding the Meta Oversight Board (https://about.fb.com/news/tag/oversight-board/ accessed 4 May 2023).

4. STATE RESPONSIBILITY FOR, AND DIRECT ACCOUNTABILITY OF PLATFORMS

Challenges of accountability for the service, products, and infrastructure were discussed at some length. The discussion covered both the accountability to which private actors should be held, but also the responsibility of governments and regulators to devise and enforce accountability regimes. Workshop participants felt that the the Minderoo Centre of Technology and Democracy evidence principle on transparency did not go far enough.[12]

Accountability was related to the necessity of researchers, regulators, and courts having access to data, and how there is no effective legal mechanism by which to compel companies to provide access to their data and systems. Specifically, the issue of access to training data (mainly for the purpose of training AI) through the copyright exception for text and data mining (TMD) in the European Union was mentioned,[13] and how often trade secret protection was used as a rationale by corporate actors to deny access.[14]

Workshop participants found that the tendency to divide accountability and liability into categories based on the size of Internet companies or online platforms, or on perceived risk to be unhelpful and out of touch with reality.[15] Participants expressed concern that such conceptual fragmentation did not reflect the interconnected

[12] Digital issue 5: Core principle 1: "All data-processing systems should be transparent" (MCTD evidence report, p. 12).
[13] See for example Martin R.F. Senftleben, *Study on EU copyright and related rights and access to and reuse of data* (European Commission, March 2022) (https://op.europa.eu/en/publication-detail/-/publication/5c5153a4-1146-11ed-8fa0-01aa75ed71a1/language-en/format-PDF/source-search accessed 4 May 2023); Christina Angelopolous, *Study on EU copyright and related rights and access to and reuse of scientific publications, including open access* (European Commission, June 2022) (https://op.europa.eu/en/publication-detail/-/publication/884062d5-1145-11ed-8fa0-01aa75ed71a1/language-en/format-PDF/source-262356864 accessed 4 May 2023).
[14] Sharon K. Sandeen and Tanya Aplin, 'Trade Secrecy, Factual Secrecy and he Hype Surrounding AI' in Ryan Abott (ed.) *Research Handbook on Intellectual Property and Artificial Intelligence* (Edward Elgar 2022).
[15] e.g. the UK Online Safety Bill (*supra* note 5) and the European Union's forthcoming AI Act (Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (COM/2021/206 final) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206 accessed 4 May 2023.

nature of the supply chain and was likely to result in confusion and be a drain on regulators and courts' resources.

5. DIGITAL COMMONS AS A PUBLIC GOOD

Workshop participants consulted the General Secretary's Common Agenda report to determine what was meant by the phrase "the digital commons as a global public good."[16] Participants found that as the digital commons was conceptualised as a public good, the digital issue was one of 'ownership' and in particular access to the digital commons as a resource.[17] In terms of international law framing and the role of states as protectors of the commons, workshop participants pointed to governance models for the Internet which would regard the Internet as a shared resource.

Workshop participants highlighted that in relation to the digital commons as a public good, then the last principle of the the Minderoo Centre of Technology and Democracy evidence report regarding the need for framework was the most important, but it also begged the question of which frameworks? In that regard, the workshop referred repeatedly to the European Union as being a leader in devising and adopting legislation in the digital, network environment, and that these frameworks were likely to be exported globally due to the 'Brussels effect.'[18]

The discussion circled back to the first digital issue of connectivity and workshop participants found that it was not enough to simply guarantee access to the Internet if people could not avail themselves of the benefits. To paraphrase one workshop

[16] *Common Agenda* (*supra* note 1) p 62.
[17] Workshop participants pointed out that the MCTD evidence report on digital issue 7, core principle 1, commitment 5 should change to no longer refer to the right to freedom of speech but to the digital good instead (MCTD evidence report, p. 15).
[18] Anu Bradford, 'The Brussels Effect' 107(1) 2012 Northwestern U Law Rev; Columbia Law and Economics Working Paper No. 533.

participant, it is not enough to guarantee access to the digital commons if people do not have the means to exploit it. Thus, it was suggested that the first principle regarding the digital issue of connecting all people to the Internet could include a right to 'equal access with equivalent benefit to all.'

MINDEROO

CENTRE FOR TECHNOLOGY & DEMOCRACY

Alison Richard Building
7 West Road
Cambridge CB3 9DT

www.mctd.ac.uk

minderoo@crassh.cam.ac.uk