Joint submission to the Global Digital Compact on targeted surveillance

- i) Core principles that all governments, companies, civil society organisations and other stakeholders should adhere to; and
- ii) Key commitments, pledges, or actions that in your view should be taken by different stakeholders governments, private sector, civil society, etc.

i) Core Principles

Civil society, researchers, activists, and journalists have revealed in multiple instances how states' use of unlawful surveillance tools <u>violates human rights</u>, including among others the right to privacy, the rights to freedom of assembly and association, and the right to freedom of expression. Furthermore, the private surveillance industry has been facilitating those abuses and has been allowed to <u>operate in the shadows</u> unchecked. Hence, states have failed in their obligations to respect as well as to protect people from these human rights abuses.

Where surveillance is operated without adequate legal frameworks, transparency, oversight, and effective safeguards, its harms have an impact far beyond those who may have actually been targeted. In the face of opacity and inadequate safeguards, human rights defenders and journalists are forced to self-censor for fear of being persecuted for their work, even if they may not be the target of such surveillance. This can be referred to as a 'chilling effect' - where people refrain from exercising their rights out of fear they could be subject to unlawful surveillance. The differentiated and intersectional impacts of unlawful surveillance on vulnerable or marginalised communities, including women and LGBT groups, is particularly egregious.

As noted in recent reports by UN human rights experts and the High Commissioner for Human Rights, the capabilities of digital surveillance tools offered on the global market are enormous. For example, they can allow "complete and unrestricted access to all sensors and information on infected devices, effectively turning most smartphones into 24-hour surveillance devices, accessing the camera and microphone, geolocation data, e- mails, messages, photos and videos, as well as all applications." (HCHR report, A/HRC/51/17, para 7) As such they permit states remote access to systems and therefore potentially to all of the data stored on those systems, including the most private information. Hacking also permits governments and other state authorities to conduct novel forms of real-time surveillance as well as the manipulation of data. The reported uses of the tools have been abusive and arbitrary, and do not constitute a permissible interference with the right to privacy. Further, states' unchecked deployment of these tools does not meet the tests of legality, necessity, and proportionality as outlined under international human rights law.

Too often, states abuse the concepts of national security or combating serious crime as a pretext for the widespread targeting of HRDs. As the UN Special Rapporteur on Counter-Terrorism has <u>noted</u>: "In recent years, the widespread misuse of surveillance technology purportedly in service of counter-terrorism and national security objectives, with concerning disregard for fundamental human rights protections, has been exposed in dramatic fashion." The PEGA Committee of the European Parliament, in their <u>draft report</u>, similarly lamented that "Member State authorities have referred to 'national security' as justification for the use of spyware and for absolute secrecy and lack of accountability."

A culture of impunity specific to targeted digital surveillance has developed that must be urgently countered. Our rights and the security of the digital ecosystem as a whole depend on it.

b) Key Commitment/ Pledges/ Actions

We urge all states to urgently take the following steps:

- 1. Immediately put in place a moratorium on the sale, transfer, export, servicing and use of spyware technology until such time as an adequate system of human rights safeguards is in place. This call has been backed by seven former and current UN Special Rapporteurs¹ and the UN High Commissioner for Human Rights².
- 2. Adopt and enforce a legal framework requiring private surveillance companies and their investors to conduct human rights due diligence in their global operations, supply chains and in relation to the end use of their products and services.
- 3. Adopt and enforce a legal framework requiring transparency in acquisition and use of surveillance technologies by both public actors and private surveillance companies.

Fernand de Varennes, Special Rapporteur on minority issues; Irene Kahn, Special Rapporteur on freedom of opinion and expression: https://www.ohchr.org/en/press-releases/2023/02/spain-un-experts-demand-investigation-alleged-spying-programme-targeting

Mary Lawlor, Special Rapporteur on the situation of human rights defenders; Clement Nyaletsossi Voulé, Special Rapporteur on the rights to freedom of peaceful assembly and of association: https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening

E. Tendayi Achiume, Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance 2017-2022: https://www.ohchr.org/en/press-releases/2021/10/special-rapporteur-contemporary-forms-racism-calls-moratorium-use

Fionnuala Ní Aoláin, Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism:

https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-onglobal-regulation-ct-spyware-technology-trade.pdf

2022 Report of the Office of the United Nations High Commissioner for Human Rights, *The right to privacy in the digital age:* https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/442/29/PDF/G2244229.pdf?OpenElement

¹ David Kaye, Special Rapporteur on freedom of opinion and expression 2014-2020: https://www.ohchr.org/en/press-releases/2019/06/un-expert-calls-immediate-moratorium-sale-transfer-and-use-surveillance

² Michelle Bachelet, UN High Commissioner for Human Rights 2018-2022: https://www.ohchr.org/en/statements/2021/09/committee-legal-affairs-and-human-rights-parliamentary-assembly-council-europe?LangID=E&NewsID=27455;

- 4. Ensure that all private surveillance companies domiciled in their countries, including sales intermediaries, affiliates, holding companies, or other investors, are required to act responsibly and are held liable for adverse human rights impacts.
- 5. As a condition to continued operation of surveillance companies, demand immediate establishment of independent, multi-stakeholder oversight bodies for private surveillance companies.
- 6. Establish community public oversight boards to oversee and approve the acquisition or use of new surveillance technologies, with powers to approve or reject based on the states' human rights obligations, provisions for public notice and reporting.
- 7. Reform existing laws or introduce new ones that provide remedy for victims of unlawful surveillance and ensure that both judicial and non-judicial paths to remedy are available in practice.
- 8. Ensure that national security laws are not misused to justify undue restrictions on access to information on the sale, transfer, export, servicing, and use of surveillance technologies.
- 9. Implement procurement standards restricting public contracts for surveillance technologies and services to only those private surveillance companies which demonstrate that they respect human rights in line with the UN Guiding Principles on Business and Human Rights and have not facilitated or contributed to human rights abuses.
- 10. Participate in key multilateral efforts to develop robust human rights standards that govern the development, sale, use and transfer of surveillance capabilities and equipment, and impose limitations as to who can be targets of digital surveillance.
- 11. Inform securities exchanges and financial regulators of the harms associated with private surveillance technology companies, and require strict, regular scrutiny in law and regulation of disclosures and applications by those companies and their owners

Furthermore, before considering the lifting - in part or in whole - of the moratorium, states must have in place appropriate legal frameworks and safeguards capable of proving that there is no tangible risk of the technology being used by purchasers, or reasonably foreseeable end users, in breach of international human rights law.

SIGNATORIES

Organisations:

- Abraji (Brazilian Association of Investigative Journalism)
- Access Now
- AfricTivistes
- Amnesty International

- Article 19
- Association for Progressive Communications (APC)
- Asociatia pentru Tehnologie si Internet ApTI (Romania)
- Bahrain Institute for Rights and Democracy (BIRD)
- · Bits of Freedom
- Business & Human Rights Resource Centre
- Center for Democracy & Technology
- CIVICUS
- Comisión Mexicana de Defensa y Promoción de los Derechos Humanos
- Committee to Protect Journalists (CPJ)
- comun.al, Digital Resilience Lab (Mexico)
- CyberPeace Institute
- Digital Empowerment Foundation
- Digital Rights Foundation
- Digitale Gesellschaft Schweiz (Digital Society Switzerland)
- Državljan D / Citizen D
- European Center for Not-for-Profit Law (ECNL)
- FMA Foundation for Media Alternatives (Philippines)
- Free Expression Myanmar (FEM)
- Front Line Defenders
- Fundacja Panoptykon (Panoptykon Foundation)
- · Global Network of People Living with HIV
- Global Voices Advox
- Heartland Initiative
- Hiperderecho
- HRDC "Memorial"
- Human Rights House Foundation
- iLaw (Thailand)
- InternetBolivia.org Foundation
- Internet Freedom Foundation
- Media Foundation West Africa (MFWA)
- Nothing2Hide (N2H)
- OpenArchive
- OVD-Info
- Pollicy (Uganda)
- · Privacy International
- Ranking Digital Rights
- Red en Defensa de los Derechos Digitales (R3D)
- Reporters Without Borders (RSF)
- Robert F. Kennedy Human Rights
- Roskomsvoboda
- SocialTIC
- Statewatch
- SUPERRR Lab
- Sursiendo, Comunicación y Cultura Digital

- Surveillance Technology Oversight Project (S.T.O.P.)
- TEDIC
- the Egyptian Initiative for Personal Rights (EIPR)
- Women of Uganda Network (WOUGNET)
- Xnet
- 7amleh The Arab Center for the Advancement of Social Media