27 March 2023

**TO: States participating in the Summit for Democracy 2023**

**ATTN: The co-organisers of the Summit—President Biden, President Chaves Robles, Prime Minister Rutte, President Yoon Suk-yeol and President Hakainde Hichilema**

**Joint Statement: States & investors have a responsibility to curtail the abuse of spyware**

We, the undersigned organisations and individuals, call on the governments convening the Summit for Democracy 2023 to prioritise human rights due diligence for spyware technologies on the Summit's agenda. We have witnessed and reported on how spyware has been repeatedly used to silence journalists, surveil human rights defenders, muzzle dissent, suppress freedom of expression of minorities, target LGBTQ+ persons and women, intimidate academia and discourage peaceful protests. To achieve greater transparency, accountability, peace and a more prosperous future for all, in alignment with the stated objective of the Summit, states and investors must act to prevent the proliferation and abuse of spyware.

The unlawful and arbitrary use of spyware has a direct and often disproportionate impact on the right to privacy and degrades other human rights and civic freedoms.[1] For example, NSO Group's Pegasus spyware is linked to at least 300 acts of physical violence in more than 45 countries worldwide. Women, LGBTQ+ persons and other vulnerable communities targeted by spyware face distinct risks of social exclusion, physical, psychological and sexual violence.

Companies have haphazardly sold and exported hacking technologies, impacting democratic processes, deepening authoritarian rule, and degrading human rights around the world (with some companies evading export licenses all together). Of the cases that have come to light, at least 14 world leaders, government officials and allies have also been identified as potential targets, putting their security and rights at risk. Investors, too, increasingly recognise that the human rights risks related to these technologies represent a material risk to their portfolios and they have an ethical, normative and fiduciary responsibility to address them. This is further evidenced by the fact that shareholders from some of the largest tech companies filed proposals on various human rights issues at the upcoming 2023 Annual General Meeting season and during the past 2022 Annual General Meetings season. **The bottom line is that states and investors, including venture capital (VC) firms, have a critical role and shared interest in preventing the abuse of spyware.**

Since 2017, the world's largest 50 VC firms (three quarters of which are domiciled in the United States) have collectively raised 309.2 billion USD, which is larger than the GDP of most countries. Early-stage investors ultimately influence which tech startups receive funding and which ideas

[1] Including, but not limited to, freedom of expression, freedom of the press, peaceful assembly, civic participation, the right to life, liberty and security of person, freedom from arbitrary arrest and detention, freedom from torture, inhumane treatment or being forced into exile, and the right to an effective remedy.

are deemed worthy of developing. **VC firms help shape the future of technology, and with it the future of our economies, politics and societies, and the realisation of human rights**.

In accordance with the United Nations Guiding Principles on Business and Human Rights, VCs have a responsibility to undertake human rights due diligence when investing in spyware due to the scope, severity of impact and low likelihood for remedy when the technology is abused. VCs, particularly those based in the Global North, must address the imbalance of power that spyware imposes on at-risk communities within their own countries and those in the Global South. This entails taking steps to identify, prevent, mitigate, remedy and account for human rights impacts through meaningful stakeholder engagement with affected communities—including during the iterative phases of product development prior to deployment.

**However, there have been very few public responses and disclosures from technology investors about their human rights due diligence practices to prevent these abuses, and those that invest in spyware are even more opaque about their procedures**. The responses that civil society has received rarely address the salient human rights risks at hand.

States have an obligation to regulate the spyware industry, as well as their investors, to prevent and mitigate human rights harms. States must therefore strengthen the collective enforcement of legal, operational and financial impacts for spyware companies who operate outside of international human rights standards. Towards this aim, we recommend that states:

- Ban the sale of spyware until a system of safeguards is in place to prevent human rights abuses and hold companies liable for their negative human rights impacts. Increase assistance, both preventative and reactive, for at-risk groups who are targeted by spyware, including human rights defenders.
- Ensure that all companies, including VC firms, domiciled in their countries are required to undertake human rights due diligence in respect of their global operations and investments. The same should apply for companies that seek to do business within their domestic jurisdictions. This includes comprehensive transparency requirements for investors, including public disclosures from VCs about their investments.
- Ensure that all companies, including VCs carry out stakeholder engagement with a wide range of actors, especially those most impacted by their products and services including at-risk individuals in the Global North and those disparately impacted in the Global South, to understand the implications of their investments and evolve their practices.
- Ensure that government agencies carry out effective human rights due diligence as a , especially surveillance-tech and cybersecurity companies.
- Hold corporate entities, including VC firms, accountable for human rights abuses that amount to criminal behaviour. Commit to cooperating in good-faith investigations about the abuse of spyware in other jurisdictions.

The shape of our economies, politics, and societies should not be founded on the technology sector's prioritisation of short-term profits, particularly when it blurs the longer-term vision of securing human rights for all. This is only possible if there is greater international pressure on companies and investors, in particular for VCs and others in the private equity ecosystem, including limited partners (LPs), to acknowledge the impact that their investment decisions have on human rights and the lives of people. Spyware poses too great a threat to not be prioritised.

As civil society organisations and individuals who have been tracking the impacts of spyware and/or engaging with companies and investors on the topic of human rights due diligence in the technology sector, we remain available for further dialogue and assistance.

Signed:

1. 7amleh: The Arab Center for the Advancement of Social Media
2. Access Now
3. Acción Constitucional
4. ALQST For Human Rights
5. ALT Advisory
6. Amnesty International USA
7. Association for Civil Rights (ADC)
8. Cambodian Center for Human Rights
9. Center for the Studies of Law, Justice and Society- Dejusticia
10. Centro de Estudios en Libertad de Expresión (CELE)
11. Centro per la Cooperazione Internazionale (CCI) / OBC Transeuropa
12. Collaboration on International ICT Policy for East and Southern Africa (CIPESA)
13. CyberPeace Institute
14. Data Privacy Brasil Research Association
15. Derechos Digitales
16. Digital Defenders Partnership
17. Digital Freedom Fund
18. Digital Rights Foundation
19. Empower
20. European Center for Not-For-Profit Law (ECNL)
21. FairSquare
22. Front Line Defenders
23. Fundación Acceso
24. Gulf Centre for Human Rights (GCHR)
25. Heartland Initiative
26. Hiperderecho
27. IMPARSIAL (the Indonesian Human Rights Monitor)
28. International Civil Liberties Monitoring Group
29. International Corporate Accountability Roundtable (ICAR)
30. International Service for Human Rights
31. Internet Freedom Foundation
32. IPANDETEC

33. Media Matters for Democracy
34. Montreal Institute for Genocide and Human Rights Studies
35. Open MIC
36. Open Net (Korea)
37. Paradigm Initiative (PIN)
38. Ranking Digital Rights
39. Red en Defensa de los Derechos Digitales (R3D)
40. SMEX
41. TEDIC
42. Thai Netizen Network
43. The Business & Human Rights Resource Centre
44. The WHRDMENA Coalition
45. Unwanted Witness
46. Usuarios Digitales