AMNESTY INTERNATIONAL

June 3, 2021

Mr. Chanan Weissman
Director for Technology and Democracy
National Security Council
White House

Re: Amnesty International policy recommendations re technology and human rights

Dear Mr. Weissman:

On behalf of Amnesty International and our more than 10 million members and supporters worldwide,[1] we write to outline our policy recommendations that address the risks posed by emerging technology and the surveillance-based business model of Big Tech.

Amnesty Tech is a global collective of advocates, researchers and technologists dedicated to:

- bolstering social movements in an age of surveillance;
- challenging the systemic threat to human rights posed by the surveillance-based business model of Big Tech;
- ensuring accountability in the design and use of new and frontier technologies; and
- encouraging innovate uses of technology to help support human rights.

Amnesty's Silicon Valley Initiative works with companies and governments to:

1. Enforce more stringent control over the import and export of surveillance technology, including by implementing a moratorium on the sale and transfer of surveillance equipment until such time as a proper human rights regulatory framework is in place; and
2. Ban the use of facial technology for mass surveillance by law enforcement bodies.

I. Enforce more stringent control over the import and export of surveillance technology

Targeted surveillance poses a serious threat facing human rights defenders ("HRDs") globally. It is the practice of putting under surveillance specific persons who may be of interest to authorities, either remotely using digital surveillance technologies, or by following and watching them in person, or a combination of the two. State intelligence and law enforcement agencies may legitimately engage in surveillance in order to acquire information essential to protect and prevent threats to the public, so long as such

surveillance activities are undertaken in compliance with international human rights law and standards. Yet, while governments have used targeted digital surveillance to fight crime and terror, some have also used it to target HRDs.

Many governments buy the sophisticated technology enabling such surveillance from private companies. They justify the procurement of these technologies as essential for maintaining law and order. Some of these surveillance companies manufacture and sell spyware or other such tools to state actors, who have used surveillance to shrink the space for dissent by targeting HRDs, in violation of their internationally recognized human rights.

Gaps in regulation, abuses by state agents, and state and corporate secrecy make it nearly impossible to identify, prevent or seek redress for the human rights abuses caused by these attacks.

To that end, the U.S. government should:

- Implement a moratorium on the sale and transfer of surveillance equipment until such time as a proper human rights regulatory framework is put in place.
- Adopt and enforce a legal framework requiring private surveillance companies to conduct human rights due diligence in their global operations, supply chains and in relation to the use of their products and services. Private surveillance companies should be compelled to identify, prevent and mitigate the human rights-related risks of their activities and business relationships.
- Adopt and enforce a legal framework requiring transparency by private surveillance companies, including information on self-identification/registration; products and services offered; sales; and human rights due diligence, mitigation and remediation measures; as well as the requirement to produce regular transparency reports reflecting compliance with the UN Guiding Principles on Business and Human Rights ("UNGP").
- Disclose information about all previous, current, and future contracts with private surveillance companies by responding to requests for information or by making proactive disclosures.

Furthermore, governments must:

- Regulate the export of surveillance technologies to ensure:
    - Denial of export authorization where there is a substantial risk that the export in question could be used to violate human rights or where the destination country has inadequate legal, procedural and technical safeguards in place to prevent abuse. States should update export control criteria to take into appropriate consideration the human rights record of the end-user as well as the legality of the use of sophisticated surveillance

tools in the country of destination, stipulating that applications shall be rejected if they pose a substantial risk to human rights.
    - All relevant technologies are scrutinized for human rights risks prior to transfer as part of the licensing assessment.
    - Transparency regarding the volume, nature, value, destination and end-user countries of surveillance transfers, for example by publishing annual reports on imports and exports of surveillance technologies. Reform any existing legislation that imposes overly broad restrictions on disclosures of such information.
    - Encryption tools and legitimate security research are not subject to export controls.
- Implement procurement standards restricting government contracts for surveillance technology and services to only those companies which adhere to the UNGP and have not serviced clients engaging in surveillance abuses.
- Ensure international co-operation to develop robust human rights standards that govern the development, sale, and transfer of surveillance equipment, and identify impermissible targets of digital surveillance.

II. Amnesty International Calls for Ban on Use, Development, Production, Sale of Facial Recognition Technology for Identification Purposes by State and Private Sector Actors.

Facial recognition technology ("FRT") is being used widely across many kinds of applications. They can generally be categorized in one of two ways: authentication / verification (1:1), or identification (1:n).

Amnesty International views FRT for identification as a mode of mass surveillance and as such, is a violation of the right to privacy. Any interference with the right to privacy must always be legitimate, necessary, and proportionate. FRT that scans and captures data from all faces within its radius is not necessary or proportionate in any circumstance.

FRT significantly hampers the right to peaceful assembly and the right to expression. Governments are increasingly turning to FRT to police protests, festivals, and sports events. Not only is this an interference with the right to freedom of peaceful assembly, freedom of association and freedom of expression, it can create a chilling effect and seriously deter such forms of peaceful dissent.

FRT can have a disproportionate impact on marginalized groups, undermining the right to equality and non-discrimination. FRT is being used by governments to intentionally target certain individuals or groups of people based on their protected characteristics, including ethnicity, race, and gender. Discriminatory impacts are a huge risk of FRT that can exacerbate existing inequalities and further disempower already-marginalized groups and populations.

Amnesty International is calling for a ban on the use, development, production, sale, and export of FRT for identification purposes by both state agencies and private sector actors.

Amnesty's specialists on technology and human rights stand ready to brief the NSC and relevant agencies. For more information, please contact Joanne Lin at 202/281-0017 or jlin@aiusa.org.

Sincerely,

Joanne Lin
National Director, Advocacy and Government Affairs

Michael Kleinman
Director, Silicon Valley Initiative