Expert Consultation on the Practical Application of the United Nations Guiding Principles on Business and Human Rights to the Activities of Technology Companies
Submission by the Delegation of the United States of America
February 28, 2022

The United States welcomes the opportunity to share views and provide input to the Office of the High Commissioner on the practical application of the Guiding Principles on Business and Human Rights to the activities of technology companies.

1. <u>The role of States in promoting respect for human rights by technology companies</u>:

- We acknowledge our duty to protect human rights as described in the UN Guiding Principles on Business and Human Rights (UNGPs) and encourage businesses to respect human rights in line with the UN Guiding Principles on Business and Human Rights, including in the design, development, deployment, governance, use and evaluation of data-driven technologies such as artificial intelligence (AI), and to ensure these products and services are subject to safeguards and oversight.
- Secretary Blinken stated at the National Security Commission on Artificial Intelligence Conference this summer, "We've got to make sure that our companies are not inadvertently fueling authoritarian practices, whether it's in China or anywhere else."
- We remain deeply concerned with the growing misuse of surveillance technology by governments, including under vague notions or specious claims of security. Such misuse not only results in arbitrary or unlawful interference with one's privacy and undermines public trust in their governments, but stifles freedoms of expression, peaceful assembly, and association.

Export Controls and Initiatives

- We have taken concrete steps to evaluate how governments could better monitor and, when appropriate, restrict the sale and export of surveillance technologies and other technologies to those who would misuse them.

- On October 21, 2021, the Department of Commerce published a Cyber Rule that will implement the Wassenaar Arrangement's multilateral export controls on items that can be used for malicious cyber activities.
- The Cyber Rule is the product of continued and extensive engagement with multilateral partners, industry, civil society, and Congress on how to enact effective export controls over a significant suite of dual-use cyber intrusion and surveillance technologies, while avoiding potential unintended, negative consequences for the cybersecurity community.
- Additionally, on November 4. the U.S. Department of Commerce added four foreign companies to the Entity List for engaging in the proliferation and use of cyber intrusion tools contrary to the national security or foreign policy interests of the United States.
- The Department of Commerce's Entity List identifies entities reasonably believed to be involved in activities that are contrary to U.S. national security or foreign policy interests.
- This includes commercial companies that provided tools that were misused to engage in cyber activities for malicious purposes, enabling human rights abuses and repression.
- Entities on the Entity List are subject to U.S. license requirements for the export or transfer of specified items from U.S. exporters. That license is reviewed on the presumption of denial.
- Two of the four companies added to the Entity Listing were NSO Group and Candiru, based on evidence that these entities developed and supplied their Pegasus tools to governments that then used these tools to maliciously target human rights defenders, government officials, journalists, businesspeople, activists, and academics. Positive Technologies and Computer Security Initiative Consultancy PTE. LTD. were added to the Entity List based on a determination that they traffic in cyber tools used to gain unauthorized access to information systems, threatening the privacy and security of individuals and organizations worldwide.

- The United States is working with like-minded governments toward establishing a voluntary written code of conduct, around which states could pledge political support to use export control tools to prevent the proliferation of surveillance software and other technologies used to enable human rights abuses. Consultations on this initiative with

industry, civil society, academia, and other relevant stakeholders will take place during the Summit for Democracy Year of Action (2022-2023).

Funding Research

- The United States government has funded research, sometimes in collaboration with industry, on technological advances that could provide valuable data-driven functionality without infringing on human rights (e.g., privacy-protecting machine learning).
- USAID is working with external partners to better understand the tensions that arise between private sector investment in technologies and human rights, explore where incentives can be further aligned to drive responsible investments in digital technologies, and identify possible actions or initiatives that can help meet this goal.

Building a Rights-Respecting Global Tech Workforce

- The U.S. government is funding development programming that supports universities and vocational schools to advance rights-respecting approaches to technology development, design, and deployment. In addition, under the Advancing Digital Democracy initiative, announced at President Biden's Summit for Democracy in 2021, USAID plans to dedicate additional funding to development programming that will catalyze investment in and demand for technology innovation that respects human rights and mitigates digital repression. This innovation will, among other things, work in partnership with and build the capacity of technology companies, hubs, incubators, universities, and civil society in our partner countries.

Content Moderation

- We encourage businesses that host third-party content on online platforms to integrate respect for human rights in developing and applying their terms of service or other rules and policies, and to provide access to remedy when content moderation or the absence thereof contributes to human rights abuses, including through dedicating sufficient resources to ensure consistent application of a platform's terms of service across content of all languages.

- We strongly encourage such platforms to act responsibly, in line with the UNGPs, to prevent and address situations where their algorithms elevate or contribute to broader dissemination of content that either incites imminent violence or violates the platform's own terms of service and policies.
- We also encourage online platforms to provide detailed and easily understandable transparency reporting on how content is displayed, amplified, down-ranked, and removed from online platforms and to make platform data more accessible for researchers in order to improve understanding of how information moves across the online ecosystem.
- We have encouraged online platforms to work with their peers to reinforce respect for freedoms of expression and association and avoid content moderation actions that could contribute, whether intentionally or unintentionally, to the infringement of human rights and fundamental freedoms.
- We are concerned about the misuse of technology to enable gender-based harassment and abuse and the silencing effect it has on the participation of women, LGBTQI+ persons, and those from other marginalized or vulnerable groups who may be politicians, activists, journalists, or other key members of civil society. We encourage online platforms to strengthen efforts to ensure these targeted groups can express themselves freely and safely.

Multilateral and Bilateral Engagement

- The United States also promotes the protection of human rights online and offline through engagement in multilateral and multistakeholder settings as well as bilaterally with other governments. The U.S. Department of State leads a working group within the U.S.-EU Trade and Technology Council on the misuse of digital technology. Within this group we focus on four discrete topics: Internet shutdowns, protecting human rights defenders online, surveillance, and disinformation.
- The U.S. government is active in the Freedom Online Coalition, a multistakeholder effort to support Internet freedom and promote human rights online. As part of the Presidential Initiative announced at the Summit for Democracy in 2021, the U.S. government has committed to expanding the Coalition's membership and deepening the Coalition's

diplomatic efforts to address the challenges and maximize the opportunities created by digital technologies.

- The United States has made supporting free and independent media – online and offline – a critical area of focus of the Summit for Democracy. The Presidential Initiative includes commitments to help provide at-risk journalists with digital security training and to increase U.S. engagement with the Media Freedom Coalition, a multistakeholder effort to promote media freedom and the safety of journalists globally.
- The United States participates in multistakeholder efforts to increase transparency in online platforms on issues such as countering terrorism and violent extremism online, including the Organisation for Economic Cooperation and Development (OECD), which is developing a Terrorist and Violent Extremist Content (TVEC) Voluntary Transparency Reporting Framework, the Christchurch Call to Action to Eliminate Terrorist and Violent Extremist Online, and the Global Internet Forum to Counter Terrorism (GIFCT), which has an ongoing working group focused on transparency. We also work closely with the Tech Against Terrorism initiative in their efforts to assist (particularly smaller) companies with tackling terrorist exploitation of their platforms, both in partnership with these other efforts and through their own transparency reporting template. The GIFCT, for which the United States serves as an Independent Advisory Committee member, also commissioned and is implementing the recommendations in the "GIFCT Human Rights Impact Assessment Report," an independent assessment of the GIFCT's efforts by Business for Social Responsibility.

2. <u>The role of States in relation to human rights due diligence on the use of technology companies' products or services:</u>

The United States has taken several steps to ensure that tools or products from cyber-surveillance companies based in the United States are not misused abroad by end-users to undermine human rights:

Guidance

In 2020, the U.S. Department of State released Surveillance Due Diligence Guidance which provides resources to businesses wishing to conduct a human rights review of their proposed transfer of surveillance technology. A link to this guidance is featured on the U.S. Department of Commerce Bureau of Industry and

Security's webpage to encourage exporters to follow the guidance. The State Department guidance sets out criteria for technology companies to evaluate whether to proceed with a transaction, as well as safeguards to implement if a company decides to proceed with a transaction. The Department suggests that businesses use these resources when considering exports of technology that could be used by nefarious actors to commit human rights abuses.

Reporting

The Department of State has updated its annual Country Reports on Human Rights Practices, an annual catalogue of human rights conditions around the world, to include a section on concerns related to surveillance practices. This report provides valuable information to academia as well as U.S. businesses conducting human rights due diligence with respect to a possible transaction.

Export Controls

- In October 2020, the Commerce Department issued a Final Rule that expanded its authority to deny a license application for crime-control items based on the "risk" the items will be used for human rights abuses.
- As part of its commitment to put human rights at the center of U.S. foreign policy, the Biden-Harris Administration is taking action to stem the proliferation of digital tools that have been misused by certain governments for repression. This effort is aimed at improving citizens' digital security, combating cyber threats, and mitigating the risk of unlawful or arbitrary surveillance.

Government Principles on Responsible Use of Surveillance Technology

- At President Biden's Summit for Democracy in 2021, the U.S. Department of State launched an initiative to draft principles to illustrate the responsible use of surveillance technologies of particular concern by a government in accordance with democratic values and with respect for human rights. The proposed principles would establish a framework for using these technologies while respecting human rights. The principles seek to lay out guidelines for, among other things, the oversight of surveillance technologies, such as how to adequately protect user data; the need to consult with civil society and the business community; and nondiscrimination in the use of surveillance technologies. We will continue to promote human rights due diligence in the technology sector and embrace opportunities to leverage the President's Summit for Democracy and Year of Action to advance this issue.

Human Rights Impact Assessment

As part of the Advancing Digital Democracy initiative, USAID plans to work with both companies and governments to strengthen regulations and implementation of human rights impact assessment in connection with the design, development, procurement, deployment and use of data-driven technology at the country level in USAID partner countries.

3. Challenges related to the ability of State-based judicial and non-judicial grievance mechanisms to provide for accountability and remedy in case of human rights abuses relating to technology companies and potential solutions to address and/or overcome such challenges:

State-Based Non-Judicial Grievance Mechanisms

As a part of broader efforts to promote sustainable economic policies, the United States recently announced and took action toward achieving its objective to further enhance the role of the U.S. National Contact Point (NCP) for the OECD Guidelines for Multinational Enterprises, on Responsible Business Conduct. The NCP provides an opportunity to raise and resolve, through voluntary mediation, claims that a business enterprise has acted contrary to the OECD Guidelines. The Human Rights chapter of the OECD Guidelines was drafted concurrently with the UNGPs, and the two sets of standards are consistent.

Through the Summit for Democracy Advancing Digital Democracy initiative, the U.S. government also plans to support partner governments' capacity to address technology-enabled human rights abuses in their country contexts, including through capacity building for legal actors and support for national human rights institutions.

Non-State Based Non-Judicial Grievance Mechanisms

In the State Department's Surveillance Due Diligence Guidance, we include recommendations for best practice with respect to business grievance mechanisms. The guidance document, including its recommendations on grievance mechanisms, was developed in broad consultation with U.S. business and civil society. In our guidance, we recommend thorough investigations of all complaints of misuse. When a credible and significant complaint of misuse is received, the product or service should be remotely disabled, and upgrades and customer support should be limited until the investigation is complete. (Given the level of complexity of investigations involving foreign governments, the U.S. seller could consider engagement in formal or informal multi-stakeholder efforts.) Where misuse is

found, the company should follow up with the actor filing the report through a secure communication channel (if it is possible to communicate securely and avoid risking the actor's safety) to provide a remedy where possible.

4. Lessons learned and best practices to advance implementation of the Guiding Principles in the technology sector:

Best practices for technology companies to implement UNGPs:

- Reinvigorate organizational human rights policies and procedures in consultation with affected groups and relevant civil society with expertise conducting human rights due diligence and human rights impact assessments.
- Adopt robust Human Rights Due Diligence (HRDD) policies and procedures.
- Conduct audits by credible and independent third-party auditors.
- Share best practices and lessons learned by participating in international fora and conferences, such as the UN Business and Human Rights Forum and RightsCon, where multistakeholder representatives can exchange information on human rights due diligence best practices.
- Enhance transparency on due diligence practices, such as through the public release of reporting.
- Communicate, in clear and accessible terms, the rules used to moderate and amplify third party content on online platforms, how those rules are applied, what kind of appeals processes exists, and what kind of accountability there is for wrongful removal of content as well as for providing transparency reporting on the enforcement of these rules.
- Establish and maintain a grievance mechanism in line with the Department of State's HRDD Guidance.
- Regularly consult with affected groups and civil society, both during the design and development phases and after systems are deployed.
- Regularly reassess the human rights conditions in a consumer's or customer's local environment or country.

Examples of steps companies can take to improve reporting on HRDD measures:

- Report on the scope of consultations conducted with affected groups while protecting their identity and ensuring these groups are fully aware of the potential use and public disclosure of their input.
- Include information on whether and how often a human rights impact assessment is conducted and provide a high-level summary of findings.
- Provide information on whether the company conducts a human rights review of government end users' human rights records, and the criteria the company uses in determining when it will turn down sales for human rights risks.
- Provide background on how the company assesses diversion/misuse risk, and the safeguards the company puts in place to mitigate that risk.
- Explain how the company can modify products or services to mitigate the risk of misuse. (This includes stripping certain capabilities from the product prior to sale; limiting the use to the authorized purpose; limiting upgrades, updates and direct support; providing for data minimization; and preventing interconnected products from being misused).
- Provide information on whether the company includes robust human rights safeguard language in contracts and if the company shares that language through transparency reporting.
- Include details on whether the company has adopted access and distribution mechanisms that allow it to maintain full control and custody of the product and cut off access as necessary.
- Provide detailed information on human rights due diligence training given to staff.
- Publicly report on the company's grievance mechanism.