From: Dickinson, Timothy L.
To: "jinny.choi@americanbar.org"; "mrios@carey.cl"
Subject: R&R regarding moratorium on the sale of commercial cyber surveillance technology
Date: Friday, April 14, 2023 12:34:10 PM
Attachments: 2023.04.13 NSO Letter to ABA International Law Section.pdf

---

This material is distributed by Paul Hastings LLP on behalf of NSO Group. Additional information is available at the Department of Justice, Washington, DC.

Hi Jinny, with apologies, I am resending the correspondence from yesterday with the addition of the header for FARA purposes. Please circulate this version. Thanks

****

Hi Jinny, attached is a letter from the general counsel of NSO, an Israeli company which has a strong interest in the above captioned R&R. As counsel for the company and a member of the SIL Council, I would like to be sure that this is included in the materials for the upcoming Council meeting.
Marcos, I would also like to be sure that there is time for me to speak to this issue when it comes up on the agenda after others have made comments. Happy to discuss before the meeting if that would be helpful.
Jinny, please let me know that you got this and it will be distributed with other Council materials.
Many thanks.

Received by NSD/FARA Registration Unit 04/14/2023 2:00 PM

NSO GROUP

April 13, 2023

Marcos Ríos
Chair, International Law Section
American Bar Association

Re: **Proposed ABA Resolution on the Sale of Commercial Spyware in the United States**

Dear Mr. Ríos:

We are in receipt of the ABA's report to the House of Delegates and proposed resolution calling for a moratorium on the sale, purchase, and use of commercial spyware pending the creation and implementation of a robust international regulatory framework governing the industry ("the Resolution"). This letter is to provide the Council with information relating to NSO's approach toward the responsible use of commercial intelligence technology, which can assist law enforcement agencies in lawful investigations to protect the security and safety of citizens against terrorism and major crime.

The Resolution proposes a wholesale moratorium on the sale of commercial intelligence technology pending establishment of a robust international regulatory framework. This blanket moratorium fails to consider the potential harms and practical impact that such a ban would have on combating terrorism and major crime. We fully support a robust international regulatory framework but oppose this Resolution. In the alternative, we would suggest that the Council consider a modified resolution allowing for the nuances experienced in the real world and permitting a pragmatic solution for legitimate and vetted purposes, similar to President Biden's March 2023 Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security (the "Executive Order"). We also propose an exception to the ABA's proposed moratorium to account for companies with an established human rights compliance program working with legitimate law enforcement and intelligence agencies, who have been successfully leveraging this technology to thwart terrorism and major crime.

1. The Moratorium Harms the Interests of United States Citizens and Allies.

The ABA's proposed Resolution to adopt a wholesale moratorium on the sale, purchase, and use of commercial spyware by federal, state, local, and tribal governments and subsequent disgorgement of any profits generated in the United States would have a direct adverse effect on the U.S. and U.S.-allied government customers. The proposed moratorium will deny the law enforcement agencies of these governments access to the tools necessary to combat identified, suspected individuals misusing end-to-end encryption in pursuit of terrorism and other serious

Received by NSD/FARA Registration Unit 04/14/2023 2:00 PM

crimes.[1] These targeted cyber intelligence tools, developed at the request of government agencies, directly address criminal and terrorist encryption methods that enables these individuals to circumvent traditional wiretaps. Additionally, these cyber intelligence tools are distinct from mass surveillance technology and only leverages data from predetermined, specified targets suspected of terrorism or other major crimes. The moratorium on the sale of commercial intelligence tools in the United States does not sufficiently account for balancing the competing interests in the use of these tools, which are essential to ensuring public safety and defending the rule of law.

The U.S. government also continues to grapple with the balance between protecting citizens' privacy and their safety. In particular, the Executive Order allows for certain exceptions and does not contemplate a wholesale ban on the use of commercial intelligence technology. Instead, the Executive Order prohibits the use of commercial intelligence technology only where government agencies "determine, based on credible information, that such use poses significant counterintelligence or security risks to the U.S.G. or that commercial spyware poses significant risks of improper use of foreign governments."[2] The difficulties in balancing the conflicting priorities of governments for the safety of its citizens and their right to privacy is further demonstrated in recent *New York Times* reporting on the FBI's procurement of NSO technology, including Pegasus.[3]

A moratorium would consequently run the risk of driving government agencies toward cyber intelligence companies operating in countries not impacted by exposure to the proposed U.S. sanctions or the disgorgement of profits requirement.[4] While we fully support the effort to develop a regulatory framework to govern the sale and use of commercial intelligence technology, we fear that a moratorium would leave the industry dominated by companies operating with less regulation, less oversight, and less motivation to respect human rights, including companies operating from Russia and China.

---

[1] Parliamentary Joint Committee on Law Enforcement, Commonwealth of Australia, *Impact of New and Emerging Information and Communication Technology*, 25 (April 2019) (addressing the impact of end-to-end encryption on criminal activity and the inability of law enforcement to monitor and respond to threats against the public). https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/NewandemergingICT/Report (explaining challenges faced by Australia's law enforcement and regulatory bodies to "undertake criminal investigations" due to increasing use of end-to-end encryption) (citing Dep't of Home Affairs, Attn'y Gen. Dep't and Australian Border Force, *Submission 28*, pp 6 and 9)).

[2] Exec. Order No. 14,093, 88 Fed. Reg. 18957 (Mar. 30, 2023).

[3] Mark Mazzetti, *A Front Company and a Fake Identify: How the U.S. Came to Use Spyware It Was Trying to Kill*, N.Y. Times, (April 2, 2023) (reporting on the FBI's procurement of Pegasus), https://www.nytimes.com/2023/04/02/us/politics/nso-contract-us-spy.html.

[4] *See* Office of the Director of National Intelligence, Annual Threat Assessment of the U.S. Intelligence Community 28 (Feb. 6, 2023), https://www.intelligence.senate.gov/sites/default/files/documents/unclassified_2023_ata_report.pdf (noting that "authoritarian states use spyware and other digital means to conduct transnational and individual critics and diaspora communities to limit their influence over domestic communities" utilizing "monitoring and threats" and that "Beijing has demonstrated its willingness to enlist the aid of China-based commercial enterprises to surveil and censor PRC critics abroad.").

Received by NSD/FARA Registration Unit 04/14/2023 2:00 PM

NSO GROUP

2. Law Enforcement and Intelligence Agencies Consider Pegasus an Essential Tool to Combat Major Crime.

NSO designs its products for the sole and legitimate use by vetted law enforcement and intelligence agencies to assist these government entities in the course of conducting lawful investigations. Our goal is to help states protect the security and safety of their citizens by licensing Pegasus to legitimate law enforcement and intelligence agencies to monitor specific, pre-identified mobile devices, similar to a traditional wiretap.

In particular, Pegasus allows these entities to: (1) monitor illicit activities of previously identified criminal actors on an individual basis; and (2) combat a core issue facing legitimate law enforcement—the misuse of encryption by terrorists and criminals to conceal plots and messages when using mobile devices. Use of Pegasus technology, for example, has thwarted numerous major terrorist attacks, captured criminal organization operatives, dismantled drug trafficking rings, aided in the capture and prosecution of pedophiles, and freed kidnapping and human trafficking victims.[5] NSO's technology is critical to the missions of legitimate law enforcement and intelligence agencies across the globe, including those allied with the United States.

3. NSO Continues to Support and Call for the Development of a Robust International Regulatory Framework for Cyber Surveillance.

NSO, like the U.S. and other governments, NGOs, and the ABA itself, recognize the risks of the unregulated sale of commercial intelligence technology. As such, we have been actively collaborating with international human rights stakeholders for the past few years to develop a regulatory framework to promote the responsible use of cyber intelligence technologies. We believe that it is critical to establish a framework to regulate our industry and establish guidelines to determine the criteria for legitimate customers of critical cyber intelligence technology. As a leading cyber intelligence company, we are uniquely positioned to actively engage key stakeholders in our industry, state agencies, and international institutions. We have gladly borne the responsibility to engage with key members to work toward establishing rules of responsible conduct and basic ground rules that states must follow to receive the benefit of this technology.

Of course, we recognize that this progress requires mobilization beyond a single company, and as such, we have been working to establish an international legal framework including sector-specific standards for states and companies, including ground rules regarding transparency, remedies, investigations, and responsibilities by each stakeholder. To drive trust and create confidence among the stakeholders on the responsible use of cyber intelligence technology, it is

[5] Ronen Bergman, *The Battle for the World's Most Powerful Cyberweapon*, N.Y. Times (Jan. 28, 2022), https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html ("Since NSO had introduced Pegasus to the global market in 2011, it had helped Mexican authorities capture Joaquín Guzmán Loera, the drug lord known as El Chapo. European investigators have quietly used Pegasus to thwart terrorist plots, fight organized crime and, in one case, take down a global child-abuse ring, identifying dozens of suspects in more than 40 countries. In a broader sense, NSO's products seemed to solve one of the biggest problems facing law-enforcement and intelligence agencies in the 21st century: that criminals and terrorists had better technology for encrypting their communications than investigators had to decrypt them. The criminal world had gone dark even as it was increasingly going global.").

Received by NSD/FARA Registration Unit 04/14/2023 2:00 PM

critical to reach a global consensus taking into account the balance between the right to privacy and the protection of states' citizens, which encompasses human rights as well

We have proposed guidance focused on widely-accepted corporate best practices for companies developing cyber intelligence technology in line with the United Nations Guiding Principles and suggested only selling to countries adhering to these human rights principles, together with mechanisms to address misuse of the system, regardless of the customer`s identity.

In our attached Concept Note, we have also outlined the basic features and principles of an international framework which covers:

- The need to balance protecting the rights of those targeted with intelligence tools with the need for legitimate use of the technology;
- The need for governments to conduct investigations with intelligence technology in a clandestine manner;
- The responsibility of service providers not to hinder the efforts of legitimate investigations;
- The need for safeguards;
- The importance of leveraging export controls as a gatekeeper for regulations; and
- The need for an independent and objective international body to conduct investigations on potential misuse.

Included in our Concept Note, we have also outlined proposed, specified best practices for human rights policies and procedures, which have already been adopted by NSO, including, but not limited to:

- Setting standards of conduct for employees;
- Ongoing monitoring and investigating potential or actual product misuse while taking into account access to necessary information and confidentiality;
- Presale due diligence;
- Investigations processes;
- Establishing trainings;
- Ensuring regular review of the policies and effective risk assessments;
- Developing consequence for violations;
- Processes for termination;

Received by NSD/FARA Registration Unit 04/14/2023 2:00 PM

- Required cooperating with ongoing investigations; and

- Ongoing grievance mechanisms.

In parallel to our efforts to promote a global regulatory framework, we developed our own human rights program that includes each of these elements. NSO continues to be one of the very few companies in our sector to have taken concrete actions to implement our commitment to human rights and have proven ourselves by not selling to customers who did not pass our rigorous Due Diligence and numerously shutting down systems, which have been misused. We are one of the only few companies in our sector engaging in open discussions with stakeholders to improve our internal processes and create transparency. Based on our experience, we firmly believe that governments, human rights organizations, and stakeholders like the ABA, can collaborate with companies like NSO to promote proper use of commercial intelligence technology.

4. Clarifications Regarding NSO and NSO Technology.

To provide additional context for our processes and the capabilities of our technology, we provide a number of clarifications with respect to NSO Group's ("NSO" or "the Company") operations in response to certain statements set forth in the Resolution. NSO has proactively implemented a number of safeguards to mitigate the impact and potential risk of misuse of its cyber intelligence technology by customers. NSO does not operate the cyber intelligence technology and licenses only to vetted law enforcement and intelligence agencies. We understand the impact of our technology and take proactive measures to call for our customers to operate in accordance with our Human Rights Policy.

- **First, NSO licenses Pegasus solely to legitimate and vetted law enforcement and intelligence agencies of sovereign, American-allied governments.** We do not permit the sale of Pegasus to any individuals or private customers. Each transaction is highly regulated by the Israeli Ministry of Defense ("MOD"), as Israel treats Pegasus as a defense article subject to extensive regulation and oversight. As such, NSO is required to undergo multiple licensing reviews in connection with each sale of Pegasus and implement requisite safeguards tailored to the unique potential risks presented by each pending customer.

- **Second, Pegasus is not an "off-the-shelf" technology. NSO has both contractual and technological safeguards and may customize each product for the specific customer, including the manner in which Pegasus is supplied.** The Resolution notes that "[s]ophisticated spyware empowers its operator to access nearly the entirety of the contents of a target's device—including private communications, notes, and photographs, as well as GPS locations and other sensitive data." We tailor the configuration of Pegasus for each specific customer and have the ability to customize limitations as set forth in our internal policies, which are consistent with the NSO Human Rights Policy. As such, we are able to limit the scope of each customer's use of the Pegasus system, which does not widely permit customers to "covertly extract contact lists, calendar entries, text and instant messages, notes, emails, search histories, and GPS locations . . . ,

Received by NSD/FARA Registration Unit 04/14/2023 2:00 PM

the smartphone's microphone and camera, and copy authentication keys," as your Resolution suggests.

- **Third, in instances of suspected misuse, NSO has shut down Pegasus remotely without accessing any of the targeted devices or the information previously collected by customers.** The Resolution notes "the use of commercial spyware by state actors raises serious concerns for human rights defenders and other individuals' rights to the freedoms of expression, association, assembly, and civic participation as well as the freedom from torture and ill-treatment." We designed Pegasus with internal segregation between various compartments, which allows NSO to terminate the entire system in instances of suspected customer misuse to target individuals in violation of NSO policies and contractual obligations.

- **Fourth, NSO contractually requires customers to represent that it strictly complies and respects Human Rights[6] and fully and strictly adheres to Human Rights norms.** The Company requires customers to adhere to NSO's human rights policies and procedures, as well as cooperate with our investigations into allegations of suspected human rights violations. As part of the customers' representations and warranties, we have included definitions in accordance with widely accepted, international human rights bodies.[7] Non-compliance with these obligations may result in immediate termination of the existing contract, and have in many cases over the last years.

* * * * *

NSO is committed to engaging in good faith with stakeholders to develop a nuanced and balanced approach toward responsible use of cyber intelligence products; collaborating on a workable solution to protect the security of citizens; and mitigating the potential misuse of technologies against vulnerable populations.

We continue to seek feedback to improve our own compliance framework and to prioritize the development of an international framework. We are happy to present our compliance efforts in this field and are ready to participate actively in a dialogue with the ABA and other organizations to establish rules of responsible conduct for this industry.

We thank you for your consideration.

[6] NSO defines "Human Rights" in accordance with widely accepted international standards as "rights contained in the International Bill of Human Rights including but not limited to the right of freedom of expression and the right for protection against unlawful and arbitrary violation of privacy."

[7] For example, our customer contracts include clear definitions of "terrorism," "national security threats," and "serious crimes."

Received by NSD/FARA Registration Unit 04/14/2023 2:00 PM

Sincerely,

Shmuel Sunray
General Counsel
NSO Group

Enclosure

Received by NSD/FARA Registration Unit 04/14/2023 2:00 PM

NSO Group Concept Note:
Proposed International Framework on the Responsible Use of Cyber Intelligence by States and State Agencies

---

I. Introduction and Background

- Over the past 18 months, legislative and regulatory bodies primarily in Brussels and Washington have held hearings, asked for public comment and received stakeholder testimony regarding the responsible use of surveillance technologies. Unfortunately, these events, often led by known cyber intelligence critics, have largely focused on allegations of misuse based on offering a decidedly one sided view of cyber intelligence technologies. For example, last year, the European Parliament established the PEGA committee, with a particular focus on the role of NSO Group and its software, Pegasus, and the use of cyber intelligence technologies by governments of EU Member States. However, cyber intelligence technologies remain in high demand with NATO-member country governments and law enforcement agencies for lawful use fighting crime and terror. Therefore, the responsible use of these critical technologies is an important topic with many implications for the broader international community.

- Cyber intelligence technologies are necessary to address international threats of terrorism and other serious crimes. The rapid development and widespread use of encryption technology by terrorists and criminals has profoundly changed the ability of states to prevent and investigate terrorism and other serious crimes. As stated by Jean-Philippe Lecouffe, Deputy Executive Director, Operations Directorate, Europol, to the PEGA committee in August 2022, "[c]riminals and terrorists are smart, they use state of the art tools to hide themselves and their communications from law enforcement" and "it is important that law enforcement can also use the accurate and updated tools and methods to prevent and fight crime and terrorism." Cyber intelligence technologies assist state authorities by addressing the "going dark" problem: the growing misuse of end-to-end encryption applications by terrorists and criminals to conceal messages and plots when communicating through mobile devices. These technologies allow for investigations without mass surveillance or a backdoor access to the devices of all users. There currently is no existing responsible alternative to cyber intelligence technologies in the hands of law enforcment and intellegience agencies, that better addresses two equally legitimate public concerns: security and privacy.

- In fact, as reflected in the recently adopted OECD Declaration on Government Access to Personal Data held by Private Sector Entities – currently, the only intergovernmental guidance on government access to privately held data – sovereign states have a duty and responsibility to protect their populations by prevening, detecting and confronting criminal activity, and government access to personal data is essential to meeting these duties and responsibilities. However, government access to personal data and cross-border data flows should be in line with democratic values and the rule of law. Access that is unconstrained, unreasonable, arbitrary or disproportionate violates international obligations, the right to privacy and other human rights and freedoms. Therefore it is important that national legal frameworks provide safeguards, and the OECD

Received by NSD/FARA Registration Unit 04/14/2023 2:00 PM

various stakeholders that would be impacted by the framework and can lend important perspectives on its development. These stakeholders could include representatives from civil society organizations, national and international governments and agencies, the private sector, and the companies developing these technologies. NSO Group would be happy to participate in such dscussions with all stakeholders to establish concrete solutions.

- The approach for building an international framework could focus on substance rather than legal form. For example, the final framework could be achieved through various legal forms, including standard setting or guidance from an international organization, such as the OECD. Ultimately, however, a non-legally binding framework is likely to bring the greatest chance of success and be more realistic for adoption.

- The mechanism by which the international framework is developed could take various forms. It could be a standalone negotiation mechanism, or it could be led by a body with the requisite experience and knowledge to lead the process. For example, the negotiation mechanism could be led by the OECD or EU, or through the appointment of another international body.

- The final international framework should be open to endorsement and subscription by all relevant stakeholders, including states, state agencies, civil society organizations, the private sector and the companies developing these technologies.

IV. Basic Features and Principles of an International Framework

i. General Overview

- An **international framework** could be developed that makes the acquisition of cyber intelligence tools subject to robust public oversight, consultation, and control, in order to comply with safeguards against illegitimate access or use, and to guarantee the principles of necessity, proportionality, legality, legitimacy, and due process.

    - The international framework and any supporting guidance to *companies* should be in line with the UNGPs, as explained further below.

    - The international framework and any supporting guidance to *states and state agencies* should be in line with the UNGPs and Principles, as explained further below.

- An international framework should also **address legitimate national security concerns**. For example, the international framework and any supporting guidance could recognize:

    - the need to balance protecting the rights of those targeted with surveillance tools (e.g., journalists, politicians, political dissidents etc.) with the need for legitimate uses of this technology when legally warranted to address international crime and national security concerns;

Adoption and endorsement of the international framework; Step 5: Monitoring and continued oversight of the international framework).

Received by NSD/FARA Registration Unit 04/14/2023 2:00 PM

Declaration, endorsed by all OECD members, provides an important international framework for guidance.

- Unfortunately, as of today, there exists no similar international framework or international guidance to regulate the cyber intelligence technology industry. Additionally, there is no national guidance provided on the foreign use of cyber intelligence, although we understand tht the U.S. government is advancing a voluntary code of conduct for surveillance technologies.

- NSO has repeatedly called for the establishment of an international framework with sector-specific standards for states and companies, and guidelines to determine the criteria for legitimate end users of critical cyber intelligence systems.

- As the most prominent global cyber intelligence company, NSO is uniquely positioned to actively engage key stakeholders among leading companies, state agencies, international institutions, and civil society organizations to establish rules of responsible conduct for the cyber intelligence industry and ground rules that states must meet to be eligible to receive exports of such technology.

- NSO offers a series of substantive ideas and proposals to establish an international framework based on principles presented in i) NSO's Position Paper, ii) the first Summit for Democracy Initiative, iii) the UNGPs and iv) other international initiatives. It is critical to develop a global consensus around the appropriate use of cyber intelligence products, and to create confidence among all stakeholders that such products are being used responsibly as intended – to make the world a safer place. In this context, NSO's understands that, within the context of the second Summit for Democracy (end of March 2023), the U.S. driven voluntary code of conduct regarding surveillance technologies and its domestic enhancements to its export control regulations will be announced.

II. The Purpose of an International Framework

- Without an international framework, regulation is effectively left to fragmented and uncoordinated national legislative efforts, which lack consistency and ridden with loopholes.

- An international framework would bring clarity and transparency to all actors, including companies, customers, civil society, and regulatory authorities.

- An international framework could address and define what constitutes legitimate use versus illegitimate use of surveillance technologies.

III. Proposing an International Framework

- An international framework could be built through a global multi-stakeholder approach.[1] This process could be the result of dialogue and collaboration across the

[1] This multi-stakeholder approach could include clear phases and steps (e.g., Step 1: Dialogue and collaboration with stakeholders for an agreed upon approach to build the international framework; Step 2: Agreement upon a negotiation mechanism; Step 3: Negotiating and drafting the substantive international framework; Step 4:

Received by NSD/FARA Registration Unit 04/14/2023 2:00 PM

- the need for governments to conduct investigations with surveillance technology in a clandestine manner;
- the responsibility of service providers not to hinder the efforts of legitimate investigations using surveillance technology;
- the need to provide safeguards for companies that follow the international framework and guidelines;
- the importance of using export controls as the main gatekeeper for regulation; and
- the need for an independent and objective international body to conduct investigations on misuse of surveillance technology.

- The international framework could be developed through a **multi-stakeholder approach**. As discussed above, these stakeholders could include representatives from civil society organizations, national and international governments and agencies, the private sector, and the companies developing these technologies.

- The international framework could establish general ground rules regarding **transparency** for companies, states, and state agencies, as explained further below. This guidance could recognize that there are legitimate legal and operational needs for secrecy of sovereign intelligence and law enforcement agencies. However, it could also recognize that cyber intelligence technologies can also be used in authoritarian states to violate the human rights of individuals. Any guidance could aim to balance these interests.

ii. Guidance and Sector-Specific Standards for Companies

- The framework could additionally include **guidance on corporate best practices** for companies developing cyber intelligence technology to mitigate risks of human rights violations through misuse of such technology and to comply with the international framework.

- This guidance should be in line with the UNGPs, including the corporate responsibility to respect human rights.

- As supported by NSO, this guidance could recommend that companies sell technologies only to those countries that have adhered to the **OECD Declaration on Government Access to Personal Data held by Private Sector Entities** or that committ to its general principles. The guidance should further invite non OECD countries to adhere to the Declaration and invite the OECD secretariat to promote the Declaration with regard to non OECD Countries.

- Informed by NSO's ongoing efforts to mitigate human rights risks, such guidance could address best practices such as:

Received by NSD/FARA Registration Unit 04/14/2023 2:00 PM

- Establishing robust internal policies, such as a human rights compliance policy, and implementing procedures;

- Implementing supporting procedures, including human rights due diligence procedures; and

- Maintaining responsible product design and appropriate safeguards to address potential misuse and downstream impacts.

- The framework could consider specific recommendations and best practices, per the above. For example, a public-facing human rights compliance policy (the "Policy") could encompass these key requirements:

  - Clearly defining "human rights violations" and "misuse," including examples;
  - Setting standards of conduct for employees, business partners, and customers;
  - Analyzing potential and actual human rights violations;
  - Incorporating all applicable international human rights laws and legislation;
  - Monitoring reports of misuse by civil society stakeholders;
  - Conducting pre-sale due diligence for customers;
  - Including customer contract provisions requiring adherence to the Policy, and requiring customers to provide notifications on actual or potential misuse that may result in human rights violations;
  - Building processes for monitoring and investigating potential or actual product misuse while taking into account the issue of providing access to the necessary sensitive information to conduct such investigations and the privates sector's limited ability to act as an arbitrator in these matters;
  - Establishing systems and technologies to support effective governance of product use (e.g., controls authorizing use, segregating duties, and allowing recording, monitoring, alerting, logging, storing and retrieving information on surveillance use);
  - Building processes for customers to report Policy violations;
  - Ensuring grievance mechanisms for external and internal whistleblowers without fear of retaliation;
  - Prohibiting modification, transfer, or third-party use of technologies,
  - Setting forth processes and guidelines for contract termination;
  - Establishing trainings for relevant stakeholders on the Policy;
  - Ensuring regular review of the policy with quantitative and qualitative performance indicators and sector-wide benchmarks;
  - Developing internal mechanisms for reporting violations of the Policy, with guidelines of consequences for violations;
  - Building processes for addressing and remedying misuse revealed by internal investigation and authorizing suspension of technology use;
  - Publicly publishing information on the Policy's effectiveness, objectives, practices and procedures; and
  - Requiring cooperation with governmental and international investigations of misuse.

- The international framework could establish ground rules regarding the provision of **remedies** when appropriate.

Received by NSD/FARA Registration Unit 04/14/2023 2:00 PM

- The international framework could provide guidance for corporate **transparency**, balancing the legitimate legal and operational needs for secrecy of sovereign intelligence and law enforcement agencies as customers.

- In addition to a general international framework, **sector-specific standards** could be considered for companies.

iii. Guidance for States and State Agencies

- The international framework could recommend that states implement national legal frameworks in line with those outlined in the **OECD Declaration on Government Access to Personal Data held by Private Sector Entities**.

a. National Laws

- The international framework could require states to **establish legal and policy frameworks at national levels** that make the acquisition of cyber intelligence tools subject to robust oversight, consultation, and control, in order to comply with safeguards against illegitimate access, and to guarantee the principles of necessity, proportionality, legality, legitimacy, and due process.

- The international framework could require states to **review and reform existing relevant laws and regulations** governing the import, export, procurement, development, oversight, sale, transfer, servicing, and use of targeted surveillance technologies in order to ensure compliance with international human rights law and norms.

- This guidance should also be in line with the UNGPs, including the state duty to protect human rights and access to remedy. It could cover the following points:

  - Legality[2]
  - Legitimate Aim[3]
  - Necessity[4]
  - Adequacy[5]
  - Proportionality[6]
  - Competent Judicial Authority[7] [8]

[2] According to Principles: Any limitation to human rights must be prescribed by law and subject to period review by legislative or regulatory processes.
[3] According to Principles: State laws permit surveillance only to achieve legitimate aims corresponding to legal interest necessary in a democratic society, applied on a non-discriminatory basis.
[4] According to Principles: Laws, regulations, activities, powers and authorities for surveillance when it is the only necessary means to achieve legitimate aim, or the means least likely to infringe on human rights.
[5] According to Principles: Surveillance must be appropriate to the legitimate aim.
[6] According to Principles: to surveillance, must establish surveillance is proportional (as defined under Principles) to a competent judicial authority.
[7] According to Principles: Determinations must be made by an impartial and independent judicial authority.
[8] Note, however, that NSO Group encourages that determinations may also rest with other regulatory and administrative bodies that are considered impartial and independent as defined under international human rights law (see relevant ECHR decisions and international guidance).

Received by NSD/FARA Registration Unit 04/14/2023 2:00 PM

- Due Process[9]
- User Notification[10]
- Transparency[11]
- Public Oversight[12]
- Integrity of Communications an Systems[13]
- Safeguards for International Cooperation[14]
- Safeguards Against Illegitimate Access[15]

- The international framework could also provide ground rules for states and state agencies regarding **transparency** and the provision of **remedies** when appropriate.

b. Clarifying Legitimate Use of Surveillance

- The framework could additionally include **guidance and examples on legitimate use of surveillance** for law enforcement and national security purposes, to comply with the international framework.

- The framework's guidance could include **determining criteria for legitimate end users** of surveillance system.

- The framework could recognize and embrace fundamental principles of human rights law, while recognizing that surveillance measures are justified where they are necessary and proportionate to achieving a legitimate goal.

c. Export Controls

- The international framework could aim to address the issue of authoritarian government misuse of technology and promote a positive vision for cyber intelligence technologies, anchored by democratic values. With this goal in mind, the international framework could provide guidance for states to **address export controls**. We understand the U.S. government is considering enhancements to its export control regulations to integrate human rights considerations.

[9] According to Principles: Requires States to ensure procedures governing interference with human rights exist in law, are consistently practiced and available to the public.
[10] According to Principles: Those surveilled could be notified by the authorizing authority with enough time and information to challenge the decision, seek other remedies, and have access to the materials in the application for authorization. Delays in notifications are justified in only limited circumstances, including if the notification would seriously jeopardize the purpose of the request, or there is an imminent risk of danger to human life.
[11] According to Principles: States could be transparent on surveillance laws, regulations, activities, power or authorities, and publish aggregate information (e.g., requests approved/rejected for surveillance).
[12] According to Principles: States could establish an independent oversight mechanism for transparency and accountability. It could access all potentially relevant information, assess legitimate use and state transparency, publish period reports, and make public determinations on lawfulness of actions. This is in addition to any oversight already provided by another branch of government.
[13] According to Principles: States could not compel service providers or hardware or software vendors to build surveillance or monitoring capability into their system or collect information purely for surveillance purposes.
[14] According to Principles: In mutual legal assistance treaties, States could apply whichever state laws on surveillance provide a higher level of protection for individuals.
[15] According to Principles: States could enact legislation criminalizing illegal surveillance by public or private actors, with civil and criminal penalties, protection for whistleblowers and avenues for redress.

Received by NSD/FARA Registration Unit 04/14/2023 2:00 PM

- Guidance on export controls could be in line with the proposals of the Export Controls and Human Rights Initiative, which was announced and supported by states having participated in the Summit for Democracy in December 2021.[16] Specifically, this would include establishing a voluntary, nonbinding written code of conduct, which like-minded states could politically pledge to use export control tools to prevent the proliferation of surveillance technologies used to enable serious human rights abuses.[17]

  We understand that the second Summit For Democracy could issue voluntary code of conduct for governments.

[16] These aligned governments committed to working to establish a voluntary code of conduct for states to use export control tools to prevent the proliferation of technologies used to enable serious human rights abuses. This initiative was announced by the U.S. Government, made in conjunction with Australia, Denmark, and Norway, and supported by Canada, France, the Netherlands and the U.K.

[17] Additional encouragement may be given to states in line with the goals of the Export Controls and Human Rights Initiative, including: (i) coordination and engagement across governments, industry leaders and academics, (ii) policy alignment across states, (iii) the strengthening of domestic legal frameworks, and (iv) sharing information on threats, risks and best practices.

Received by NSD/FARA Registration Unit 04/14/2023 2:00 PM