NSO, Pegasus and Human Rights

Introduction

The rapid development and widespread use of technology has profoundly changed the ability of states to prevent and investigate terrorism and other serious crime, bringing great challenges as well as opportunities. The use of new technologies by terrorists and criminals to further their unlawful activities has, in turn, required intelligence and law enforcement agencies to search for and embrace new technologies to combat terrorism and other serious crime. Of particular concern is the impact and potential risk of misuse of technology and how to balance legitimate security concerns with respect for human rights and, in particular, the right to privacy.

This position paper summarizes essential background information on "Pegasus" and NSO Group Technologies ("NSO")'s human rights program, and sets out proposals for how society should collaborate to regulate the sector and better mitigate potential harms caused by NSO's technologies while still benefiting from the protections they provide.

NSO was founded in 2010 with the ambition to make the world a safer place. Its mission was – and remains – to assist lawful investigations by state authorities to protect the security and safety of citizens against major crimes and terrorism, thereby contributing to the enjoyment of human rights. NSO's products are licensed and provided to government intelligence and law enforcement agencies to fight crime and terror. In particular, NSO's products help state authorities address the "going dark" problem: the growing misuse of encryption by terrorists and criminals to conceal messages and plots when communicating through devices.

NSO is most well-known for "Pegasus", a technology used by states and state agencies around the world to collect data from specific mobile devices of suspected major criminals. As terrorists and criminals routinely further their criminal activities by misusing end-to-end encryption to communicate and conspire securely, Pegasus remains a technology essential to combatting terrorism and other serious crimes and to defend the rule of law. NSO's technology enables state authorities to penetrate the cloak of secrecy concealing targeted criminals and dismantle sex-, drug- and human-trafficking rings, tackle pedophilia rings, locate missing and kidnapped children, rescue survivors from collapsed buildings and protect the security of airspace.

A clear illustration of severity of the risks posed to children online by inaccessible encrypted services, for example, is highlighted by the WeProtect Global Alliance, which brings together governments, the private sector, civil society and international organizations to develop policies and solutions to protect children from sexual exploitation and abuse online. The organization's 2019 Global Threat Assessment identified:

> *"Publicly-accessible social media and communications platforms (as) the most common methods for meeting and grooming children online. In 2018, Facebook Messenger was responsible for nearly 12 million of the 18.4 million worldwide reports of CSAM [child sexual abuse material] to the US National Center for Missing and Exploited Children. These reports risk disappearing if end-to-end encryption is implemented by default, since current tools used to detect CSAM do not work in end-to-end encrypted environments."*

Received by NSD/FARA Registration Unit 05/24/2022 10:04:20 AM

In their 2021 Assessment, WeProtect Global Alliance restated the urgency of the situation. Their findings confirmed that the risks posed to children online have continued to grow and diversify as *"[e]ven offenders with minimal technical ability can evade detection by using easily accessible encrypted messaging services and anonymity tools."*[1]

Similarly, Australian legislators have acknowledged the "going dark" problem posed by end-to-end encrypted messaging. Indeed, this is one of the main challenges for intelligence and law enforcement agencies in today's highly digitized world and dynamic environment. A 2019 report prepared by Australia's Parliamentary Joint Committee on Law Enforcement, for example, noted:

> *"The challenges to law enforcement posed by criminal activity 'going dark' are significant and ongoing. As the implementation and uptake of encryption increases, including through the use of entirely legal infrastructure such as 5G networks, the impact on law enforcement's capacity to detect and disrupt cyber and cyber-enabled crime will only be exacerbated."*[2]

NSO's Pegasus technology has enabled state authorities to thwart numerous terrorist attacks and has been instrumental in apprehending terrorists and other serious criminals operating clandestinely in the cybernetic world. As stated in the New York Times Magazine (Jan. 31, 2022):

> *"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."*

It is clear that any given technology is not inherently good or bad. Pegasus is a technology designed and provided to contribute to the fight against major crime and, therefore, the protection of human rights. But, like any other technologies, it can also be misused to violate human rights. The same is true of end-to-end encryption – a technology that can contribute to the respect of human rights, including the right to privacy, but can also be misused by criminals responsible for severe human rights violations.

In fact, the Pegasus system allows for targeted surveillance only, with customers purchasing a limited number of licenses for concurrent targets, and is therefore less intrusive when compared with a backdoor. This concept was recognized in a recent interview featuring Belgian Minister of Digitalisation and Privacy Mathieu Michel, who expressed disagreement with:

---

[1] WeProtect Global Alliance, 2021 and 2019 Global Threat Assessment Reports, available at https://www.weprotect.org.

[2] Parliamentary Joint Committee on Law Enforcement, Commonwealth of Australia, Impact of New and Emerging Information and Communication Technology (April 2019), available at https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/NewandemergingICT/Report.

Received by NSD/FARA Registration Unit 05/24/2022 10:04:20 AM

> *"[L]owering the level of security and privacy of all Belgians' messages . . . to conduct investigations from time to time. It's as if, because the police and the justice system do searches from time to time, everyone should leave their back door open . . . today we have technological means to access tapping other than by degrading the level of security of all Belgians. Look at the Pegasus software."*

NSO is fully aware of and committed to its own human rights responsibilities and the duties of its clients, and is determined that its products be used appropriately and lawfully. Any allegation that Pegasus has been misused by a state or state agency to wrongly target anyone – including a journalist or human rights defender – is extremely concerning. Any such allegation immediately triggers a thorough review process and investigation into the reported claims. NSO is not afraid to take decisive action, such as terminating the contract with a customer, when necessary. Moreover, as a highly regulated company, NSO may only pursue customer relationships within the constraints imposed by Israeli law, including the Israeli government's own set of human rights protections.

NSO is also aware that progress requires a mobilization beyond an individual company. The United Nations Guiding Principles on Business and Human Rights ("UNGPs"), for example, specifically note that "[s]tates do not relinquish their international human rights law obligations when they privatize the delivery of services that may impact upon the enjoyment of human rights."[3] Continuing dialogue, including multi-stakeholder exchanges and multilateral efforts that encompass governments, industry, academic communities, and civil society, therefore remains key to appropriately regulating this sector to best ensure proper respect for human rights. NSO is uniquely situated, as the sector's pioneer with more than 60 clients in 45 countries across different continents, to contribute to such discussion.

This is why NSO:

- Reiterates its strong support for the establishment of an international legal framework and sector-specific standards for states and companies. This is critical to guide and regulate the use of surveillance tools by states and state agencies for legitimate law enforcement and national security purposes. Such a framework would also establish ground rules regarding transparency and the provision of remedy when appropriate.

- Welcomes the *Export Controls and Human Rights Initiative* to help stem the tide of authoritarian government misuse of technology and promote a positive vision for technologies, anchored by democratic values. This initiative was announced by the United States, Australia, Denmark and Norway and is further supported by Canada, France, the Netherlands, and the United Kingdom. NSO is fully prepared to engage with these countries and others, as well as with any other international organizations or stakeholders.

- Renews its standing invitation to all stakeholders, including civil society organizations, states, international organizations and the United Nations Special Procedures, to engage in a meaningful dialogue with a view to establish concrete solutions to promote respect for human rights by all.

[3] United Nations, Guiding Principles on Business and Human Rights, available at https://www.ohchr.org.

Received by NSD/FARA Registration Unit 05/24/2022 10:04:20 AM

Better Understanding Pegasus

While substantial public attention has been drawn to Pegasus, it remains poorly understood. It is important to underline that it is designed – and can only function – to collect intelligence from specific mobile devices. The technology is more limited in scope than public reporting suggests:

- It is used with specific, pre-identified phone numbers, one at a time;
- In many ways, Pegasus is similar in concept to a traditional wiretap. Instead of listening to specific conversations, it helps law enforcement monitor mobile messaging, offering legitimate law enforcement and intelligence operations personnel a window into the activities of previously identified and targeted criminal actors on an individual basis;
- Pegasus does not delete or edit data on a targeted device or allow for such deletion or editing;
- Pegasus cannot be used to gather information broadly and does not penetrate computer networks, desktop or laptop operating systems or data networks;
- Pegasus is not a mass surveillance technology and only collects intelligence from the mobile devices of specific, pre-identified individuals.

In addition, NSO does not operate this technology. NSO licenses Pegasus to law enforcement and intelligence agencies of sovereign states and government agencies, following a careful and sector-leading pre-engagement due diligence process (see NSO's Due Diligence Procedures set out in Annex 1 below). Licenses are limited in number and contracts are carefully crafted to permit only legitimate use.

For good reason, and a core tenet of NSO's corporate ethics since it was founded, NSO does not have any knowledge of the individuals whom states might be investigating, nor the plots they are trying to disrupt. Sovereign states normally do not, will not, and should not, share this extraordinarily sensitive information with NSO or any other provider of similar technology.

NSO is constrained in its ability to say more about its customers, the crimes prevented and criminals tracked and apprehended using its technology, as a result of the legitimate legal and operational need for secrecy of sovereign intelligence and law enforcement agencies.

Received by NSD/FARA Registration Unit 05/24/2022 10:04:20 AM

Three Myths Surrounding Pegasus

Myth 1: NSO operates Pegasus and collects information about the individuals it is used against.

- **Fact**: NSO licenses Pegasus to sovereign states and state agencies, does not operate Pegasus, has no visibility into its usage, and does not collect information about customers.

Myth 2: Pegasus is a mass surveillance tool.

- **Fact**: Data is collected only from the mobile devices of specific individuals, suspected to be involved in terrorism and other serious crime, subject to judicial or other appropriate oversight.

Myth 3: Pegasus can delete or alter data stored or shown on an individual's phone.

- **Fact**: Pegasus is not capable of creating, editing or deleting data on a mobile device. Instead, the software enables states to access and collect data stored on a device.

The NSO Challenge

As the UN High Commissioner for Human Rights restated on July 19, 2021, surveillance measures are justified where they are necessary and proportionate to achieving a legitimate goal. NSO recognizes and embraces the fundamental principles of human rights law, notably ICCPR article 4, which requires states not to derogate from their obligations with respect to certain human rights under any circumstances. These rights include the right to life, freedom of thought, conscience and religion, and freedom from torture or cruel, inhuman or degrading treatment. Similarly, NSO recognizes that derogation from other rights is only permitted in the special circumstances defined in international human rights law: any such measures must be of exceptional character, strictly limited in time and to the extent required by the exigencies of the situation, subject to regular review, consistent with other obligations under international law and not be discriminatory in any way.

Because NSO's technology is exclusively provided to and operated by states and state agencies, it is inherently challenging to ensure that states fulfill their primary duty not to violate human rights through the misuse of NSO's technology. To mitigate the risks and provide concrete solutions, in 2019 NSO adopted an upgraded human rights due diligence procedure. This procedure, which was presented in detail in the 2021 *NSO Group Transparency and Responsibility Report,* is summarized in Annex 1. The NSO Due Diligence Procedure is based on ex-ante, during and ex-post controls and verifications on both the customer and the use of Pegasus. The human rights due diligence program:

- Has identified the most salient human rights risks associated with NSO products, and is tailored to prioritise mitigating these risks. This includes working to prevent misuse against journalists, members of civil society organizations, lawyers and dissident politicians and campaigners.

- Includes pre-engagement due diligence building upon data on states' human rights performance and track record independently provided by credible civil society organizations and incorporates objective scoring and filtering, subjective research and analysis, internal independent supervision and external government oversight – to properly mitigate the risk of providing products to a state authority that might misuse them.

- Involves licenses that define and permit only legitimate uses, require compliance with NSO's Human Rights Policy, include bespoke restrictions as appropriate and ensure enforcement rights for NSO.

- Established, maintains and operates internal and external whistleblowing policies, accommodating confidential and anonymous reporting, which trigger the product misuse investigation procedure.

- Prioritises customer and client training and, increasingly, is embracing transparency despite the legitimate confidentiality constraints inherent in this area of work.

- Is developed and continuously improved with key input from an external panel of experts and in light of stakeholder feedback, and implemented and enforced in partnership with NSO's external lawyers around the world.

NSO is proud to be the first and to its best knowledge the only company in the cyber industry that is implementing policies towards complete alignment with the United Nations Guiding Principles on Business and Human Rights.

While NSO is constantly working to improve its policies and practices to further mitigate the risk of misuse, this endeavor takes place in a context in which we as a society are lacking best practices and guidance both for states to appropriately balance their essential law enforcement and crime prevention efforts with their human rights obligations and for the industry's responsibility to respect privacy and human rights.

This is why NSO has highlighted the need for an international legal framework and sector-specific standards, as well as guidelines to better determine criteria for legitimate end users of crucial surveillance systems. This is critical to guide and regulate the use of such invasive tools by states and state agencies for legitimate law enforcement and national security purposes, and to establish ground rules regarding transparency and the provision of remedy when appropriate. Achieving this is beyond the scope of private companies' efforts alone, and properly requires the direction and oversight of a democratic and public political process.

Accordingly, NSO is highly supportive of the export controls and human rights initiative announced and supported by states having participated in the Summit for Democracy in December 2021. NSO stands ready to engage constructively in this process as well as to any other international process or initiative.

NSO Reaction to the "Pegasus Project" Reports and NSO's Next Steps

Beginning in July 2021, a number of allegations against NSO were published in a series of "Pegasus Project" reports from "Forbidden Stories" ("the Report"). Despite the fact that many of these allegations have proved to be baseless, misrepresented and false, NSO

nonetheless takes them seriously. As with all allegations of misuse, NSO has followed these steps:

- Investigate each and every allegation related to an existing customer,
- Continuously improve its human rights program, including through provision for or cooperation in the remediation of human rights harms,
- Continue to engage with all stakeholders, and
- Support the development of international standards.

Investigating Allegations

The original allegation that the "list" contains details of individuals "selected as people of interest by clients of [NSO]" – does not purport to implicate Pegasus or any NSO technology. The editor of the *Washington Post*, a member of the Report consortium, conceded that "the purpose of the list could not be conclusively determined" and that "it is unknown how many of the phones were targeted or surveilled". Additionally, Amnesty wrote that they "never presented this list as 'NSO's Pegasus Spyware List', although some of the world's media may have done so". This nuance and caveat have been conspicuously absent from most reporting of the allegations, resulting in coverage that, whether deliberately or not, was (and remains) misleading, speculative and sensationalist.

Despite these serious shortcomings and material inaccuracies, NSO always takes extremely seriously all allegations that its products may have been involved in any human rights adverse impact.

To address, properly and fully, the allegations reported, NSO immediately started a thorough review process and launched investigations into the reported claims.

More specifically, and even if some actions cannot be made public in light of legally binding national security restrictions and confidentiality obligations, NSO has undertaken appropriate steps, including the following:

- Suspended customers' use of the system,
- Conducted detailed reviews of domestic legal frameworks,
- Reviewed relevant contracts and agreements,
- Interviewed end-users and legal representatives to understand processes, protections and perspectives, and
- Verified facts from objective sources.

In some cases, NSO has reinstated the system after gaining comfort that the technology was not misused. In other cases, it has fully severed relationships with customers after misuses were identified. Some cases are still under active investigation, including instances where NSO is awaiting the outcome of various government-level inquiries being conducted in parallel.

Received by NSD/FARA Registration Unit 05/24/2022 10:04:20 AM

NSO is able and willing to cooperate with any official state inquiry into the use of its products by any customer agency of that state, and, indeed, NSO has done so successfully in the past. NSO can also participate in any inquiry by an international organization, provided that the confidentiality restrictions mentioned above are addressed. Such cooperation could facilitate disclosure and potentially the provision of remedy by the state to any victim of human rights violations.

Continuously Improving NSO's Human Rights Program

As NSO has consistently stated, including prior to the widespread reporting related to the "Pegasus Project" and the recent interest from several governments, NSO is committed to fully implementing the United Nations Guiding Principles on Business and Human Rights and the OECD Due Guidelines.[4]

While NSO is the first company in its sector to undertake such public commitments, NSO is not complacent nor will it wait passively for the adoption of a much-needed international framework for the industry globally. Instead, NSO is redoubling its own efforts to continuously enhance its human rights program and mitigate risks; and to address states' legitimate concerns.

NSO has begun work on designing and implementing the following initiatives:

1. Reviewing product design options for incorporating stronger human rights safeguards, including the viability and effectiveness of establishing "whitelists" of mobile devices and identifying out-of-scope surveillance activities;

2. Reviewing NSO governance frameworks and the potential for enhanced engagement of independent experts;

3. Further enhancing NSO's human rights due diligence procedures, including mechanisms to reduce the potential misuse of products in connection with journalists, to be developed in discussion with civil society organizations, academics and policymakers;

4. Reviewing the feasibility of developing an audit process for gathering data regarding customer use and proactively assessing compliance mid-contract;

5. Promoting improved access to effective remedies for victims, including by increasing options in contract terms and pursuing legal action against customers responsible for product misuse and adverse human rights impacts;

6. Reviewing and updating legacy contracts, in light of substantiated concerns communicated by states, to ensure long-standing customer relationships meet the same human rights standards and are subject to the same contractual safeguards as new engagements; and

7. Enhanced training of customers to ensure proper compliance with contract obligations.

---

[4] United Nations, Guiding Principles on Business and Human Rights, available at https://www.ohchr.org; OECD, Due Diligence Guidance for Responsible Business Conduct, available at https://www.oecd.org/investment/due-diligence-guidance-for-responsible-business-conduct.htm.

Received by NSD/FARA Registration Unit 05/24/2022 10:04:20 AM

NSO welcomes the opportunity to discuss these and other possible enhancements to its human rights program.

Engaging Stakeholders

NSO is committed to engagement with stakeholders to more fully understand, allay and/or act upon concerns relating to human rights risks. To be clear, NSO is ready and willing to engage in good faith with any credible independent expert, including human rights defenders and others from civil society organizations, representative organizations, companies, or other groups, even if the feedback is critical.

NSO hopes that this readiness and willingness is reciprocated as it believes that robust engagement is essential to improving mutual understanding of the risks and challenges associated with balancing the state duty to protect the physical security of its individual populations with the potential misuse of technologies against dissidents, vulnerable populations, and others.

Over the past year, NSO has engaged and sought to engage with numerous stakeholders, receiving useful – and sometimes pointed – feedback and commentary on its human rights program and approach. Many of the suggestions and recommendations have been integrated into NSO's framework. Examples include sources that are now used as part of NSO's due diligence procedures, how NSO might consider enhancing transparency in relation to issues and incidents despite the inherent limitations that exist in this sector, and the integration of additional international standards into NSO agreements. These suggestions help to strengthen processes, and further mitigate risks of misuse and potential adverse human rights impacts by NSO customers.

Supporting International Standards

In addition, NSO actively supports efforts to create standards and mandate further transparency in the cyber intelligence world. NSO has actively promoted engagement around responsible product design and usage in its sector that balances the need for legitimate law enforcement activities with the risk that state actors misuse cyber intelligence products against journalists, civil society, dissidents and political opponents, and vulnerable populations.

NSO is ready to participate actively in dialogue with and within international organizations, in the hope that further engagement among leading companies, state agencies, international institutions and civil society organizations will help establish rules of responsible conduct for this industry and ground rules that states should meet to be eligible to receive exports of such technology. NSO fully understands and indeed expects that some of those rules could require adjustments to its business approach, and even perhaps cause negative commercial consequences. Nevertheless, NSO's steadfast desire is to help 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 as intended making the world a safer place.

****

Received by NSD/FARA Registration Unit 05/24/2022 10:04:20 AM

Annex 1

NSO'S HUMAN RIGHTS DUE DILIGENCE PROGRAM
(As of May 2022)

Our Main Human Rights Risks

Through our legal and human rights-focused analysis of our products and new developments, investigations, engagements with third parties and customers, and review of third party reports, we have identified the most salient human rights risks associated with our products. These include:

- The potential misuse of our products against people and groups that act to promote or protect human rights in a peaceful manner ("human rights defenders"). These include: (i) journalists; (ii) members of civil society organizations; (iii) lawyers; and (iv) political parties, candidates and supporters.

- The potential misuse of our products for reasons unrelated to national security or law enforcement, such as in support of litigation or to obtain information that may be embarrassing to individuals.

- The use of our products by unauthorized personnel associated with states and state agencies, which is at odds with our agreements and enhances the risks of negative impacts.

- State use of our technology in a manner inconsistent with human rights norms. For instance, there may not be judicial or other independent approval processes, and when they do exist, we have identified situations where the process or protocols for obtaining approval, standards against which approvals should be judged, and/or requirements for documenting the reasoning associated with granting approvals, may not be fully transparent.

- State use of our technology authorized by regulations regarding surveillance that may lack: (i) a definition of the nature of offenses that may legitimately lead to surveillance, and categories of people who may be surveilled; (ii) a limit on the duration of surveillance activities; (iii) a clear procedure to be followed when examining and using information obtained; (iv) precautions when communicating gathered information to other parties; and/or (v) circumstances in which information may be destroyed.

- These impacts can result, and in some cases we believe have resulted, in violations by our customers of several fundamental human rights. These include the right to privacy, the right to freedom of expression, and the right to freedom of assembly. Potential violations of these rights also represent the most severe, least remediable, most widespread and most likely adverse human rights impacts that could arise from customer misuse of our products.

- There is a wide variety of additional government-driven risks that could flow from our technologies. These could include rights associated with the legal and judicial process, such as freedom from arbitrary arrest and detention and similar abuses or improprieties in the legal process, as well as invasions of freedom of thought,

Received by NSD/FARA Registration Unit 05/24/2022 10:04:20 AM

conscience and religion, restrictions on freedom of movement, or participation in civic life.

We keep this assessment of our company's salient human rights risks under review.

Human Rights Due Diligence

NSO's human rights due diligence is a vital part of our corporate strategy, enterprise risk management and responsible business conduct. This is especially true when it comes to licensing tools that, if misused, could potentially have serious adverse human rights impacts. We cannot ultimately prevent a state misusing our technology, but we can and do ensure that we are very selective with respect to the identity of the countries and customers with which we are willing to do business in order to mitigate the risk of such misuse.

We adopted our Human Rights Due Diligence Procedure (the "HRDD Procedure") in April 2020 to further implement our Human Rights Policy and to help the company comply with applicable local laws, international norms and human rights principles. The HRDD Procedure requires the assessment of potential human rights impacts prior to the sale of our products to each customer, paying particular attention to potentially vulnerable groups. We believe our process is best practice and compares favorably with the larger defense industry.

In high-level summary, our HRDD Procedure encompasses several components:

Initial Filter

Based on an in-depth review of various compliance concerns, we have decided upon a list of more than 55 countries to which we do not and will not sell cyber intelligence products, for reasons such as human rights, corruption, and regulatory restrictions.

Opportunities from these countries are not brought to the management committee for consideration and are rejected even before the due diligence process shall be initiated.

Initial Risk Assessment and Classification

NSO's internal compliance team conducts a two-part evaluation of human rights risks associated with any new business opportunity: a country assessment, followed by analysis of the specific opportunity.

First, we generate a numerical country assessment score using a carefully curated and annually reviewed (and, if necessary, updated) list of external and widely respected rankings, indicators and other data from sources including: the Economist Intelligence Unit; Fund for Peace; Vision of Humanity; Freedom House; Transparency International; the World Bank Worldwide Governance Indicators; Trace International; and CIVICUS.

Then, we classify the risks relevant to the specific opportunity by examining: (1) the degree to which the specific product(s) could adversely impinge upon the human rights of targeted individuals; (2) the degree to which there is a perceived potential adverse human rights impact; (3) reputational risks; (4) where the product(s) would be used; (5) the relative authority and governance of the prospective customer organization; and (6) other factors. The opportunity evaluation must include a review of the product type and capabilities, customer organization type and mission, and proposed duration of relationship.

NSO's Vice President for Compliance combines the country score and the opportunity classification to reach an initial risk rating of "elevated", "moderate" or "low". This risk rating determines the level of due diligence conducted during the next stage.

Information Gathering and Assessment

The diligence process relies on information gathered from a number of sources, including: denied parties checks; results of media searches in English and local languages; information from NSO employees; information about the domestic legal framework; information about the prospective customer; input from relevant government authorities; and reports from partners and external risk and investigative firms.

The due diligence requirements for each risk classification can be illustrated as follows:

	Risk/Source	Low	Moderate	High
Open Source Intelligence	Results of internal adverse media country and End-User overview research	✓		
	External risk and investigation firm, report to include publicly available information and adverse media country and End-User overview, human rights and foreign policy		Level 1	Level 2
Human Intelligence - Questionnaires	Sales Manager	✓	✓	✓
	Activity reports – Onsite and Client Executives [N/A for renewals]	✓	✓	✓
	Support [N/A for new End-User]		✓	✓
	Partner	✓	✓	✓
	Investigation firms		Level 1	Level 2
	Government input (strategy)			✓
Legal Framework	Publicly available information about local laws and legal framework		✓	
	Local legal opinion			✓
	Export Control (E.U., U.S., IL)		Level 1	Level 2
	SDN / Embargoed Countries	Level 1	Level 2	Level 2
	End User questionnaires/interviews			✓

Received by NSD/FARA Registration Unit 05/24/2022 10:04:20 AM

Final risk classification, review and approval

Review by the General Counsel of the Compliance Team's assessment memorandum.

The General Counsel can require additional due diligence to be undertaken at this stage.

When satisfied with the due diligence performed, the General Counsel determines the final risk classification: "high", "moderate" or "low".

"High" and "moderate" risk marketing opportunities (i.e., new countries without specific customer opportunities) plus all specific customer engagements are subject to Management Committee review and approval.

Enhanced Approval

Additionally, the GRCC reviews and has final approval in three circumstances: (1) for all "high" risk customer engagements; (2) where Management Committee approval was not unanimous; and (3) where the Management Committee referred the opportunity to the GRCC for consideration.

Contractual Provisions

Every customer and business partner contract requires compliance with all applicable laws and regulations, including those governing the use of our products, and international human rights norms.

Customers and their employees must also receive, understand and comply with NSO's Human Rights Policy.

Customers must undertake not to "target individuals or groups because of their race, colour, sex, language, religion, political or other opinions, national or social origin, property, birth or other status or their otherwise lawful exercise or defense of human rights".

We strictly require that Pegasus is used only where there is a legitimate law enforcement or intelligence-driven reason connected to a specific, pre-identified phone number, and after a process is followed where a state agency decision-maker independent of the user – such as a court – authorizes that use consistent with a written domestic law.

Where not clearly defined under domestic law, or where domestic law is not consistent with international norms, NSO includes contractual provisions defining specific crimes and terrorism-related activities – based on definitions in international instruments – in respect of which our products may be used.

We limit the specific crimes in respect of which – and the geographic scope within which – our products may be used, along with the duration of our agreements, where appropriate, to ensure NSO can regularly review the appropriateness of each relationship.

Customers are obliged to provide timely notice to NSO of any knowledge they may have regarding suspected misuse that may result in a human rights violation, and to cooperate with NSO investigations regarding allegations of human rights violations.

Received by NSD/FARA Registration Unit 05/24/2022 10:04:20 AM

NSO ensures we have the contractual right to suspend or terminate use of our products for human rights-related misuse.

Additional human rights-related assurances are required based on identified risks or mitigation measures, such as training requirements, certification conditions, enhanced termination rights and other measures.

Ongoing Oversight

All customers are subject to ongoing oversight for compliance with the terms of their agreements and NSO's Human Rights Policy.

Effective monitoring of customer activity is a significant challenge, since we do not have immediate insight into the use of our products. Moreover, as legitimate law enforcement agencies with a mission of protecting against terrorism and serious crime, customers operate with strict confidentiality requirements, including where required by law and/or judicial or customer procedures, and are reluctant to share information to prevent inadvertently compromising security and law enforcement activities.

Despite these challenges, we regularly engage with customers to discuss human rights and examine compliance with the terms of our agreements. We also review public information sources for reports that may suggest potential misuse.

We are always seeking additional ways to improve our approach to ongoing oversight, and some current considerations are outlined in the main body of this position paper.

We do not license Pegasus to customers where, following our HRDD Procedure, we conclude there are inadequate country-level protections (including but not limited to an insufficiently strong rule of law) in place to confidently prevent misuse. As a result of our HRDD Procedure, from May 2020 through April 2021, approximately 15% of potential new opportunities for Pegasus were rejected for human rights concerns that could not be resolved. NSO has rejected more than US$300 million in opportunities based on the outcomes of our HRDD Procedure.

Grievance Policies

NSO encourages both internal and external stakeholders to raise concerns of misconduct. Our grievance mechanisms allow both confidential and anonymous reporting. However, we encourage whistleblowers to interact directly with an assigned team of discreet investigators, including by providing information that may help substantiate allegations. NSO takes all due care to keep whistleblower information confidential, where appropriate. Our policies, for both internal and external reports, also reflect the company's commitment to protect whistleblowers from any unfair or detrimental treatment.

Internal Whistleblower Policy

Adopted in September 2019, this internal policy encourages openness and support for whistleblowers who raise concerns in good faith, and provides protection for whistleblowers from detrimental treatment as a result of raising genuine concerns.

Applies to all employees, consultants, officers, and directors.

Provides a grievance mechanism to raise concerns to the NSO's most senior management – including executive management, General Counsel, and the Vice President for Compliance – through a dedicated email account.

Though anonymous reporting is supported, interaction with investigators is encouraged, which allows for a more thorough investigation of all key facts.

Investigators are required to evaluate all reports, investigate where there is sufficient information, and conduct extensive analysis and review of credible information.

External Whistleblower Policy

Also adopted in September 2019, this promotes transparency by allowing any external person or body – including contractors, employees, partners, officers, and directors, as well as potentially affected individuals – to report a grievance through a confidential email account, which is reviewed by the Vice President for Compliance.

Encourages interaction with investigators, but provides safeguards for anonymous whistleblowers.

Once the company receives a report from a whistleblower or otherwise identifies a concern, including through media or NGO reports, NSO conducts an investigation using the framework described in NSO's Product Misuse Investigation Procedure.

Investigations

Adopted in April 2020, NSO's Product Misuse Investigations Procedure ("Product Misuse Procedure") provides a framework for responding to reports of potential product misuse. The procedure governs the timely investigation of potential product misuse – including a thorough review of potential human rights abuses – and requires consistent and swift mitigation measures when appropriate.

The procedure aims to ensure that each investigation is conducted in accordance with a number of investigative goals, including to:

- Comply with applicable laws and NSO policies, including the HR Policy,
- Respect the rights of all stakeholders,
- Determine key facts and causes,
- Perform investigations objectively and expeditiously,
- Draw appropriate conclusions, balancing the rights of stakeholders,
- Undertake appropriate remedial action, if any, and
- Preserve confidentiality of the incident reporter to avoid or minimize retaliation, if applicable.

Upon receipt of information about a potential misuse, NSO undertakes, in all cases, a preliminary review to determine whether there is sufficient information to appropriately

Received by NSD/FARA Registration Unit 05/24/2022 10:04:20 AM

investigate a potential instance of product misuse, including whether the allegation is technically feasible. The Vice President for Compliance also responds to the whistleblower, seeks any additional information necessary to conduct the preliminary review and any related investigation, and takes all necessary steps to avoid or minimize the risk of any retaliation against the reporter. The Vice President for Compliance coordinates with the Management Committee to determine how to proceed.

Following the preliminary review, the Management Committee determines whether to proceed with a full investigation and, if so, appoints an investigation team led by an attorney.

Investigations may include a review of data, interviews, meetings, and an evaluation of objective risk factors, including an analysis of whether the customer has engaged in previous human rights abuses.

NSO Compliance will evaluate information from the customer, such as information about the process followed in connection with the use of NSO products to target specific individuals, the duration of use, circumstances leading an individual to believe they were targeted using an NSO product, and customer country information.

The customer is contractually required to provide this information, which is maintained in the customer's systems logs in a tamper-proof manner. Refusal to cooperate results in the immediate suspension of the customer's right to use the system.

The compliance team will also engage in an in-depth review of media reports, open source research, analysis of domestic law and protections, customer processes, and adherence to international human rights norms.

This analysis will include a review of the legal basis for the customer's use of NSO's products, their interference with individual human rights at issue and whether the customer applied sufficient safeguards when obtaining intelligence using NSO products.

During an investigation, NSO's compliance team meets directly with our customer to ascertain: the extent of the customer's compliance with the terms of its contract; customer practices regarding compliance with the legal framework; operational protections; the customer reporting lines; responses to previous human rights abuses, if any; and the basis for interception.

Investigation results are shared with the Management Committee and the GRCC to collaboratively determine next steps and potential remediation. Depending on the outcome of the investigation, when warranted, the company will take appropriate corrective action to mitigate potential harm. As a result of the findings, the customer may be subject to corrective action ranging from retraining to termination of the relationship.

In some cases, we are unable to conclusively determine whether there was, or was not, a misuse of our products. In those instances, we develop and implement additional mitigation measures designed to prevent future misuse.

Through our experience conducting these investigations, and with recommendations from our external advisors, NSO has strengthened our initial due diligence and review processes, including by enhancing the initial assessment of domestic laws, strengthening contractual provisions, and providing human rights training for customer personnel.

However, a number of inherent challenges remain, given the nature of our customers. Because of their strict confidentiality requirements, we are unable to provide actual or alleged victims with information about adverse impacts or implemented remediation, or even acknowledge relationships with specific customers. [Currently,] even where we identify product misuse, we cannot breach these confidentiality requirements. While we cooperate with states to try to ensure that when abuses occur within their jurisdictions those affected have access to effective remedy, the confidentiality restrictions limit our ability to do much more. While we follow the approaches described in the UNGPs to the extent feasible with respect to remediation, both the UNGPs and we, ourselves, recognize that this is a complex and difficult area in particular for our sector.

Training and Communications

NSO conducts human rights trainings for employees and customers:

Employees

All new employees receive human rights training as part of their on-boarding process.

We provide staff with regular employee updates on human rights, including through the CEO's "all hands" meeting.

The company trains existing employees in key functions including sales, marketing, and those with direct relationships with customers – twice a year on human rights matters.

In 2020, the company, with support from human rights advisors, conducted approximately 18 targeted trainings focusing specifically on human rights. Some 121 participants attended these targeted training sessions.

The Vice President for Compliance also meets regularly with the company's R&D team to discuss human rights concerns, mitigating measures, and relevant questions.

Each new product is evaluated from a human rights perspective.

Customers

NSO also provides comprehensive human rights training to customers. This training includes a discussion of human rights obligations, the international framework for human rights norms, and customer responsibilities with respect to individual human rights, focusing on the right to privacy and the right to freedom of expression.

Key stakeholders are required to attend.

During 2020, approximately 127 customer participants attended the 18 human rights trainings held by NSO.

Government Oversight

Even after we have completed our internal human rights processes, we are closely regulated by export control authorities in the countries from which we export our products: Israel, Bulgaria and Cyprus.

The Defense Export Controls Agency ("DECA") of the Israeli Ministry of Defense strictly restricts the licensing of Pegasus, conducting its own analysis of potential customers from a human rights perspective.

Transparency

NSO is committed to transparency to the maximum extent possible, while necessarily we must respect our customers' critical national security considerations and our corresponding legally binding confidentiality obligations.

In June 2021, we published NSO's first Transparency and Responsibility Report. As the first company in our sector to issue such a report, we are proud that we took a large step towards greater openness by volunteering as much detail as possible about NSO's human rights program. All this notwithstanding the inherent challenges to prepare such a report, owing to our customers' critical national security considerations and our corresponding legally binding confidentiality obligations.

This report was not intended as the last word on NSO's human rights work. To the contrary, we are committed to publishing further such reports, which we hope will show that we continue to improve our systems of preventing and mitigating misuse of our products and ensuing adverse human rights impacts.

Also public is NSO's correspondence with the human rights Special Procedures of the UN Human Rights Council in recent years, in which we have sought to engage constructively on what it means to operate an effective human rights program in our sector and how NSO could contribute to multilateral and multi-stakeholder collaboration aimed at developing much-needed robust, effective, coherent and realistic sector-wide policy solutions. We hope to receive a response from the UN Special Procedures responding in equally constructive spirit to the questions, recommendations and invitation contained in our latest letter dated September 20, 2021.

We are actively exploring various possible means of reducing or overcoming some confidentiality constraints in order to further enhance our transparency. We appreciate that this is an important part of building trust with our stakeholders, identifying instances of product misuse by our customers, and enabling us to do more to ensure that victims of such misuse are provided information and access to effective remedy.

Received by NSD/FARA Registration Unit 05/24/2022 10:04:20 AM