TRANSPARENCY AND RESPONSIBILITY REPORT 2024

Contents

1 Executive Summary

In a world that is plagued by growing extremist views, crime and instability, NSO Group ("the Company" or "NSO") remains committed to developing technological solutions that protect what matters most: human lives and fundamental freedoms. Our third Transparency and Responsibility Report ("2024 Transparency Report" or "this Report") represents our ongoing efforts to balance cutting-edge technological capabilities with our commitment to continue to strengthen and enhance our human rights compliance program ("compliance program").

The events of this past year have been a powerful reminder of why our work matters. The horrific terrorist attacks in Israel; the ongoing instability in regions like Syria and the Ukraine; the rising tide of global security threats; and the surge of hate crimes in the very heart of western democratic countries all demonstrated the critical role of responsible cyber intelligence. These challenges have highlighted the need for lawful access to encrypted communications, a concern echoed by Europol's Executive Director during a recent statement. While addressing encrypted communication technology providers, she emphasized that anonymity in the digital environment should not shield criminals from justice and called for a balanced approach that ensures lawful access for combating crime while safeguarding democratic values. These principles resonate deeply with NSO's mission.[1]

NSO Group is unlike any other company that creates powerful technological tools. Our mission and responsibility reach far beyond that. We have developed and continue to actively enhance our human rights compliance program —a program that sets a new standard in the cyber intelligence industry. NSO's human rights compliance program was designed in accordance with the letter and spirit of the United Nations Guiding Principles on Business and Human Rights. To develop our compliance program, we focused intently on how our technology should be used. We understand that our work exists in a world of nuanced challenges. Authorized government agencies must simultaneously prevent terrorism, disrupt serious criminal networks, perpetrating serious and violent crimes and protect national security while vigilantly safeguarding individual rights to privacy, free expression, and personal liberty. This balance is the core of our Company's approach.

In 2024, we conducted a baseline self-assessment of our human rights compliance program using the UN Guiding Principles on Business and Human Rights (UNGP) Reporting Framework and Implementation Guidance, the Reporting Principles and the Assurance Guidance. This internal review aimed to establish a baseline for evaluating our practices. These were not mere bureaucratic or theoretical exercises, but genuine attempts to understand, improve and lead by example in an industry that demands the highest levels of ethical conduct.

Our vision extends far beyond our Company's operations. We are actively working to establish international regulatory frameworks for cyber intelligence technologies. We approach this mission with humility, eager to share our extensive experience while remaining open to learning from diverse perspectives across academic, policy, and technological fields.

The global landscape continues to present complex challenges that require sophisticated, responsible solutions. Whether it's countering terrorist communications, protecting vulnerable populations or unlocking critical intelligence to law enforcement, our technologies play a crucial role in maintaining safety and preserving democratic values.

Looking forward, we remain dedicated to continuous improvement. We will continue to invest in our human rights compliance program, engage meaningfully with stakeholders and push the boundaries of what responsible technological innovation can achieve. Our ultimate goal is to develop cyber intelligence tools that not only protect lives but also uphold the fundamental principles of human rights.

This 2024 Transparency Report is more than a record of our past efforts – it's a commitment to our ongoing mission of creating technological solutions that make the world safer, more secure, and more equitable.

[1] Suzi Ring & Laura Dubois, *Europol Chief Says Big Tech Has 'Responsibility' to Unlock Encrypted Messages*, FINANCIAL TIMES (Jan. 20, 2025), https://www.ft.com/content/1e6a600d-8620-4ed6-a4cd-5c454d6247ba.

Understanding Pegasus

- **Pegasus is not a mass surveillance tool.** It is used with specific, pre-identified phone numbers of suspected terrorists and criminals, one at a time. In many ways, Pegasus is similar to a traditional wiretap.
- **Pegasus is not operated by NSO Group.** It is licensed to legitimate, vetted intelligence and law enforcement agencies of sovereign states for prevention and investigation of terrorism and other serious crimes in accordance with applicable laws and regulations.
- **Pegasus does not manipulate existing data, or implant new information.** Pegasus is not designed to add, alter, delete, or otherwise manipulate data on targeted mobile devices.
- **Pegasus does not penetrate computer networks, desktop or laptop operating systems, or data networks.** It can be installed only on smartphones and cannot be used to gather information more broadly.

2 About NSO Group

NSO Group is a global technology company based in Herzliya, Israel. Our journey began with a clear mission: to provide governments and law enforcement agencies around the world with certain tools they need to combat terrorism, serious crime and other major threats to public safety. Today, that mission continues to guide everything we do, as we develop and license advanced cyber intelligence technologies designed to address these pressing global challenges.

In a world where threats are constantly evolving and criminal actors are becoming more sophisticated, the tools needed to protect public safety must also evolve and keep up with the technological advancements. Criminal networks, terrorists, and other malicious actors have found ways to exploit end-to-end encryption and other technologies to hide their activities, making it increasingly difficult for authorities to detect, prevent, and investigate crimes. This is where NSO Group has a critical role – our Company develops technological solutions that help legitimate government authorities keep pace with these active threats.

2.1 Why We Exist: Supporting Public Safety in a Changing World

Our core mission at NSO Group is to help make the world a safer place. This guiding principle is at the heart of all the technologies we develop. While much of the attention has been focused on our well-known product, Pegasus, our suite of solutions goes beyond any one tool. From mobile intelligence acquisition to geolocation technologies used in search-and-rescue missions, our products are built to help protect human lives.

The importance of our mission is highlighted by Goal 16 of the United Nations Sustainable Development Goals (SDGs), which aims to promote peaceful and inclusive societies, provide access to justice, and build effective, accountable institutions. We see ourselves as active contributors to this goal by providing law enforcement the means to prevent acts of terrorism and violence, dismantle criminal networks, and protect vulnerable communities.

But we are also acutely aware of the responsibility that comes with developing these powerful tools. The potential for misuse is real, and we take it seriously. We are committed to ensuring that our products are used in the most ethical way possible – i.e., only by legitimate government authorities and only for their legitimate intended purposes. That is the reason we have put in place rigorous compliance procedures and programs, which govern the development, sale, and use of our technologies. That said, we are also mindful that no technological solution can ever guarantee absolute protection against misuse.

2.2 The “Going Dark” Problem: A Growing Challenge

Adapted from the U.S. Federal Bureau of Investigation (FBI), "going dark" refers to ceasing or significantly reducing digital or electronic communication to avoid detection or monitoring, often by criminal actors, intelligence targets or other entities seeking anonymity or secrecy.

Going Dark

In 2011, Valerie Caproni, then serving as FBI General Counsel, described going dark as:

> A potentially widening gap between our legal authority to intercept electronic communications pursuant to court order and our practical ability to actually intercept those communications.

This correctly describes a critical challenge that governments and law enforcement agencies face today: the fact that criminals and terrorists increasingly use encrypted communication to disappear from view, making it harder to track their illicit activities.

While law enforcement often has the legal authority to access communications under court orders, they lack the technical capability to do so due to end-to-end encryption. This challenge is widely referred to as the “Going Dark” problem. Although encryption rightfully safeguards privacy for law-abiding citizens, it also enables bad actors to operate in secrecy, evading detection, and carrying out harmful activities. Evidence shows that criminals and terrorists have repeatedly used encrypted communication to avoid prosecution and to plan attacks. Just as criminal actors misuse technology designed to protect the privacy of individuals, our technology also has the potential to be misused.

NSO Group's mission is to help governments bridge this technological gap, providing lawful tools that enable authorities to intercept critical information in the fight against crime and terrorism, all while adhering to strict legal frameworks and human rights considerations to mitigate misuse.

2.3 The Evolution of Threats and Our Role in Countering Them

Over the last decade, the landscape of public safety threats has changed dramatically. Criminals and terrorists have become more adept at using technology – staying one step ahead of law enforcement. Encrypted messaging apps, social media platforms, and other digital communication tools have given these individuals and organizations the ability to communicate and coordinate their activities without fear of being intercepted. They can plan and execute terrorist attacks, organize drug trafficking operations and exploit vulnerable populations without leaving behind traditional trails of evidence.

This is where NSO Group has a critical role. We develop technologies designed to directly address these challenges. For example, similar to the traditional wiretap, Pegasus, allows government agencies to lawfully infiltrate the mobile devices of suspects involved in serious criminal activity, aiding law enforcement ingathering the information they need to disrupt plots, rescue victims and bring criminals to justice. Our geolocation tools have been used in critical search-and-rescue operations, enabling authorities to find missing persons quickly and effectively as well as apprehend fugitives who wish to escape the law.

2.4 Leadership and Governance: Building a Culture of Responsibility

At the heart of NSO Group is a leadership team that is deeply committed to maintaining high ethical standards.

Board of Directors

Our Board of Directors, supported by the Governance, Risk and Compliance Committee (GRCC), oversees the implementation of our policies and ensures that our commitment to human rights and ethical conduct is embedded in everything we do.

Management Committee

The Management Committee, which is comprised of our Chief Executive Officer ("CEO"), Senior Vice President of the Client Business Division, and General Counsel ("GC"), is responsible for the day-to-day execution of these policies and ensuring that our operations remain aligned with our

This strong leadership structure helps us foster an ethical company culture starting at the top – a company culture that prioritizes accountability, transparency, and integrity. We believe that creating an ethical work environment starts from the top and filters through every level of the organization. It's not just about following the rules – it's about doing the right thing, even when it's hard.

2.5 Our Products: Technology That Saves Lives

We develop and license a suite of cyber intelligence tools designed to assist legitimate law enforcement and government agencies in protecting public safety. Our technologies enable agencies to lawfully access critical information by infiltrating the mobile devices of specific individuals suspected of serious criminal activity, such as terrorists, human traffickers, or organized crime bosses.

Pegasus, has drawn significant attention due to its powerful capabilities. However, it is crucial to understand what Pegasus does and, more importantly, what it does not do.

Pegasus is a targeted surveillance system designed to be installed on a single mobile device, with strictly limited licenses and usage subject to comprehensive legal restrictions and frameworks specific to each customer's jurisdiction.

In addition, contrary to certain allegations, Pegasus does not add, alter, delete, or otherwise manipulate data on targeted devices. Moreover, Pegasus is limited strictly to smartphones. It cannot penetrate computer networks, servers, desktops, laptops, or broader data systems.

This functionality makes Pegasus analogous to a traditional wiretap, though tailored to the modern world's use cases. Pegasus provides legitimate law enforcement authorities with a narrow window into a suspect's activities for a defined period of time, and it is used solely for targeted surveillance on specific individuals who pose an imminent threat. Law enforcement agencies use Pegasus under strict domestic legal guidelines to gather vital intelligence, enabling them to thwart terrorist plots, rescue victims, and dismantle criminal networks.

Pegasus has been proven to save lives and to provide crucial data in life-or-death situations, all while respecting the legal limits imposed by government frameworks and export control laws as well as the broader principles of privacy and other fundamental civil liberties.

Additionally, Pegasus is not a mass surveillance tool. It can only be deployed on identified devices linked to specific individuals, with licenses restricting the overall number of installations. This

ensures that Pegasus is deployed responsibly and with oversight, further protecting individual privacy while addressing critical security needs.

We are a technology company that develops and then licenses software to our government end-user customers. Like other technology companies, we license the solution and provide technical support, but we do not operate Pegasus nor do we have any involvement in the specific investigations conducted by law enforcement – we never access the data collected, nor do we know who is being investigated. We merely enable law enforcement agencies to do their jobs while adhering to both local laws and international human rights standards.

2.6 Regulatory Compliance: Operating Under Strict Regulations

While we have also implemented a voluntary internal framework to prevent misuse of our products, NSO Group is also subject to stringent external regulatory oversight, ensuring that our sales and operations comply with both domestic and international standards. Given the sensitive nature of our technologies, which are classified as “defense articles”, all sales are subject to approval by the Israeli Ministry of Defense's Defense Exports Control Agency (DECA). DECA's role goes beyond mere administrative approval. It conducts its own rigorous evaluation of potential customers, including a human rights assessment to ensure that our products are sold exclusively to legitimate government agencies that have been properly vetted.

In practice, before any marketing or sales activity can commence, we must obtain the necessary export licenses from DECA for sales of Pegasus, as well as from the relevant export control authorities in other countries, such as Bulgaria for export of our tactical and network products. DECA imposes its own set of constraints, performing an independent evaluation of each customer. In certain instances, DECA has decided to reject applications for export licenses and in other cases has added terms to licenses based on Israeli foreign policy considerations. Moreover, all customers are required to sign an End-User Certificate addressed to the Israeli government, which obligates them to use our products lawfully and in compliance with international legal standards.

This multi-layered regulatory oversight not only augments our own due diligence efforts but also adds an additional safeguard to ensure the responsible use of our technology.

In some cases, even after obtaining valid export licenses, we have voluntarily terminated engagements with customers upon identifying new political, legal, diplomatic, or human rights risks through our ongoing diligence processes. This collaborative approach between our internal compliance mechanisms and external regulatory bodies strengthens our commitment to the ethical use of our technology, ensuring that our products align with global human rights principles.

2.7 Looking Forward: Innovating with Purpose

As we lo ok to the future, we remain committed to our mission of making the world a safer place. We are constantly innovating, seeking new ways to enhance our products while maintaining our ethical foundation. Our technology will continue to evolve to meet the challenges of an increasingly complex and dangerous world, but our commitment to human rights and responsible business practices will never waver.

We understand that transparency is key to building trust, which is why we are committed to regularly engaging with stakeholders, including governments, human rights organizations, and civil society. We welcome open dialogue and are always looking for ways to improve our processes and strengthen our compliance programs.

Our goal for the future is clear: to continue developing innovative technology that protects public safety, while upholding the highest standards of ethics, transparency, and accountability.

3 Our Commitment to Human Rights

Our dedication to human rights drives every aspect of our work. We align ourselves with authoritative global standards, including the UNGP, the OECD Guidelines for Multinational Enterprises and the UN Counter-Terrorism Legal Training Curriculum. These frameworks guide not just our internal operations but also how we engage with the wider world – make sure that human rights remain at the forefront of our business decisions and actions.

Building an ethical foundation

Our commitment to human rights isn't just a check the box exercise, it's a fundamental part of our identity and corporate DNA. In collaboration with world-renowned business and human rights experts, we've developed a comprehensive human rights compliance program. This program establishes clear ethical guidelines for how we operate, covering every phase of our work – from the inception and development of our products to their licensing and eventual use in the real world by our customers. But our responsibility doesn't stop with us. We hold our partners and customers to these same high standards, demanding respect for human rights at every step of the way.

Tackling risks with responsible innovation

We recognize that our technology, particularly sophisticated tools like Pegasus, carries inherent risks. These tools could potentially be misused to infringe on individuals' privacy, suppress free speech or hinder public debate. Aware of this reality, we have taken measures to mitigate these risks to the greatest extent possible. Pegasus is licensed exclusively to legitimate government bodies with the clear and lawful objective of safeguarding national security and public safety. We do not take these decisions lightly. Before licensing, we conduct human rights due diligence to ensure that safeguards are in place. Where conditions pose an unacceptable risk of misuse, we reject the sale. Our responsibility does not end there – we continue engagement with the customer both pre- and post-sale to ensure strict adherence to such our principles.

Vetting our customers

Part of our human rights strategy involves being selective about who can purchase licenses to use our products. Our vetting process goes beyond technical assessments – it includes reviews of the potential customer's track record on human rights. We examine the specific political, legal, and human rights conditions in the customer's country. If we believe that the risks are too high or the existence of safeguards is insufficient, we will not proceed with the sale. Even after licensing, our agreements impose strict limitations on how our products are used, and we require our customers to use our technology solely for lawful and legitimate purposes, such as intelligence or law enforcement operations.

Accountability and grievance mechanisms

Our grievance mechanisms and product misuse reporting channels are vital to our human rights commitment. In situations where allegations of misuse arise, we act swiftly and decisively. We launch immediate investigations, engaging independent third parties if necessary, to determine the validity of the claims. If systematic misuse is confirmed, which constitutes a breach of the customer's human rights contractual obligations, we take decisive action, including, in necessary cases, terminating the customer's access to our technology. In this way, we remain fully accountable for the impact of our products.

Learning and evolving

Since the inception of our current human rights compliance program in 2019, we have continually learned from experience and evolved our practices. We have strengthened our due diligence processes, adding layers of oversight, and polished our mitigation strategy. Our contractual safeguards have been updated to reflect the latest best practices in human rights protection. In parallel, we expanded our training programs to ensure that all employees, from technical teams to executive leadership, as well as our customers, understand their role in upholding human rights principles.

Collaborating for a better future

Our work is not done in isolation. We regularly act to engage with external human rights advisors, stakeholders, and civil society groups to gather diverse perspectives and improve our processes

and will continue to do so even if such groups are less receptive to such engagement. This collaboration, when successful, allows us to stay ahead of emerging challenges, refine our practices based on “best practices”, and develop innovative solutions that prioritize human rights. We believe that an open dialogue with these communities not only strengthens our own practices but also sets an example for the industry. We also constantly evaluate our internal policies and adapt them based on feedback, evolving legal standards, and new technological challenges, thus making sure that our human rights compliance program remains dynamic and responsive to change.

3.1 Salient Human Rights Issues

In line with the UN Guiding Principles on Business and Human Rights, NSO Group prioritizes the identification and management of salient human rights issues. These are the most severe human rights risks directly linked to our business operations and the use of our technology. Recognizing the potential adverse impacts that may arise from our products, we continuously assess, prioritize, and address these risks as part of our ongoing human rights due diligence.

Through robust product analysis, lesson learning from prior incidents, engaging with diverse stakeholders, and incorporating insights from independent third-party reports, we have identified specific human rights risks that are most relevant to our operations and the broader cyber intelligence industry.

Among these risks are the potential misuse of our technology against vulnerable individuals and groups, including human rights defenders, journalists, and civil society actors. There is also the risk of deployment for purposes unrelated to national security or legitimate law enforcement activities, including surveillance that may not align with international human rights standards. Additionally, the unauthorized use of our technology by unqualified personnel, and its use in ways that are inconsistent with both domestic laws and international norms, such as the absence of independent oversight in the approval of surveillance requests, are significant concerns.

We understand that if these risks materialize, they could result in serious violations of fundamental human rights. These include, but are not limited to, breaches of the right to privacy (as enshrined in Article 12 of the UDHR and Article 17 of the ICCPR), infringements on freedom of expression (Article 19 of both the UDHR and ICCPR), and restrictions on the right to peaceful assembly (UDHR Article 20, ICCPR Article 21). Furthermore, there is the potential of violations of due process rights, including the freedom from arbitrary detention (UDHR Articles 3 and 9, ICCPR Article 9), the right to freedom of thought, conscience, and religion (UDHR Article 18, ICCPR Article 18), as well as the freedom of movement and participation in public life (UDHR Article 13, ICCPR Article 12).

In response to these identified risks, NSO Group has taken steps to implement and operationalize a Human Rights Due Diligence (HRDD) process in line with the expectations set out in the UNGP. Our HRDD process involves an assessment of each new business opportunity, incorporating scrutiny of potential customers to ensure that our technology is not misused. This process includes assessing the legal and governance frameworks in which customers operate, as well as evaluating their commitment to upholding international human rights standards.

In 2024, we have rejected over USD 20M in new business opportunities due to human rights concerns

We recognize that despite these due diligence efforts, no process can provide absolute assurance that our technology will be used exclusively in accordance with human rights norms. This is an inherent risk around the actual use of the system when a Company is a system provider to a government agency operating in the field. Our ability to monitor the real-time use of our products is inherently constrained, particularly since our technology is deployed by government agencies. However, we attempt to mitigate this by exercising enhanced scrutiny when dealing with customers in jurisdictions where the rule of law is weak, where domestic legal frameworks fall short of international human rights standards, or where internal customer processes lack sufficient safeguards. As noted, where that risk cannot be appropriately mitigated, we reject the sale and do not engage with a customer.

Our 2024 commitment, however, goes beyond evaluating the risks associated with the use of our products.

This year, we placed a heightened focus on identifying and addressing human rights issues throughout our entire supply chain.

We recognize that human rights risks extend beyond our direct customers and include our suppliers, contractors, and other business partners, and thus addressed a broader range of human rights risks.

We have begun expanding our due diligence efforts to ensure that our suppliers operate in accordance with internationally recognized human rights standards. This involves evaluating our partners' labor practices, environmental impact, and adherence to anti-corruption measures. While these supply chain risks may be distinct from those associated with the use of our products, they remain integral to our broader human rights agenda.

Further details about our approach to addressing human rights risks in our supply chain will be discussed in a designated chapter later in this report. This chapter will outline the steps we are taking to embed human rights considerations throughout all aspects of our business, including in our entire value chain.

3.2 Key Policies and Procedures

- Over the course of the last year, we expanded our focus to include greater scrutiny of our **supply chain**. We drafted and published a Supplier Code of Conduct, setting clear expectations for our suppliers regarding ethical conduct, human rights adherence, fair labor practices, and environmental responsibility. In tandem, we introduced a Sanctions Policy to help ensure that our supply chain remains compliant with international regulations and free from unethical practices.

- Since adopting our **Human Rights Policy** in 2019, we have actively integrated the abovementioned human rights principles into our decision-making processes. To operationalize this, we have established key policies and procedures that anchor our human rights compliance program, some of which are detailed in the relevant chapters of this transparency report. **The Human Rights Due Diligence Policy** is central to our risk management efforts. It outlines a detailed process for assessing and addressing potential human rights risks both for existing customers and new business opportunities. This policy covers everything from initial risk assessments to the determination of appropriate levels of due diligence, formulation of mitigation strategies, and final approval processes. Each step is designed to minimize the risk of human rights abuses associated with the misuse of our products.

- **The Internal and External Whistleblowing Policies** provide mechanisms for reporting any suspected misconduct or risks related to our products and activities. Whether it's concerns about bribery, corruption, or the inappropriate use of our technologies, these policies help ensure that both employees and external parties can report issues confidentially and without fear of retaliation. They serve as critical tools in identifying potential human rights violations and safeguarding transparency.

- Our **Potential Product Misuse Investigation Procedure** outlines how we handle allegations of product misuse. This policy sets the standard for conducting thorough, timely, and consistent investigations, providing a structured approach to reporting findings to relevant stakeholders and taking appropriate remedial actions. The procedure ensures accountability and transparency in addressing any potential misuse of our technologies.

Together with our Code of Ethics and Conduct, which complements these policies by promoting transparency, anti-corruption measures, equal opportunity and other pillars of the Company's ethics, these policies form a holistic approach to embedding respect for human rights across all facets of our operations.

Reaching beyond the Human Rights Policy, our Code of Ethics and Conduct (CoC) extends our overall responsibility into numerous critical areas. It encompasses policies that address conflicts of interest, responsible procurement, export controls compliance, personal data protection,

environmental responsibility, and equal opportunity and inclusion. Additionally, the Company's Anti-Bribery and Corruption (ABC) policies, cover third-party engagements, gifts, hospitality, and more, ensuring all interactions adhere to the highest business integrity standards, as well as other related policies and procedures, such as Acceptable Use Policy (AUP), Anti-Harassment Policy, and others. Collectively, these policies codify our dedication to transparent and responsible business conduct.

3.3 Governance Structure

Oversight of NSO Group's human rights compliance program starts at the highest level of the organization: the Board of Directors. The board not only adopts the Company's compliance policies but also actively reviews human rights issues tied to NSO's activities. The board appointed the Governance, Risk, and Compliance Committee (GRCC), which oversees governance and human rights policies, with final authority over sales approvals, particularly for elevated-risk opportunities identified during due diligence. This includes the power to approve, reject, or impose conditions on sales to mitigate risks.

The GRCC is composed of the Company's CEO, General Counsel, an independent director, and two additional directors from the Company's group. Day-to-day management of the human rights compliance program is delegated to the Management Committee, led by the CEO and other senior executives, who meet at least monthly to review sales opportunities, internal investigations, stakeholder engagements, and compliance matters. The committee reports to the GRCC biannually, ensuring accountability and ongoing oversight.

Supporting this structure, the Vice President for Compliance leads a dedicated compliance team ("Compliance Team"). This Compliance Team oversees risk assessments, customer vetting, contract safeguards, and product evaluations from a human rights perspective. They also manage and conduct internal investigations, , and human rights training, and review whistleblower reports, collaborating closely on all the above with external advisors who provide country-specific insights, human rights expertise, and strategic guidance on long-term goals.

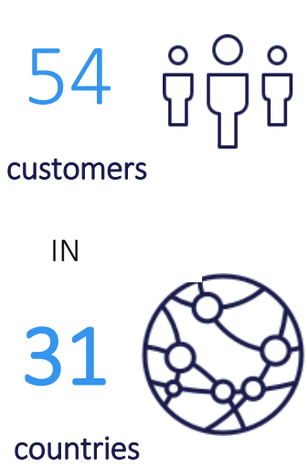
Together, these teams and processes ensure that human rights considerations are embedded across all business operations, from product development to customer engagement, reinforcing the Company's commitment to transparency, responsibility, and ethical conduct. Further details on the Company's governance and human rights practices can be found in the Company's recent Transparency and Responsibility Reports.

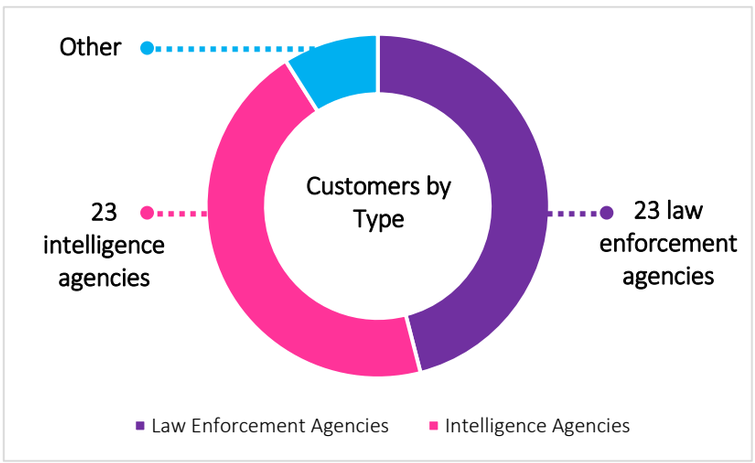
3.4 Overview of Human Rights Compliance Program

3.4.1 Human Rights Due Diligence

As part of our HRDD process, each new sales or marketing opportunity undergoes a risk assessment led by our Compliance Team. When a business function identifies a new opportunity, it submits a request to the Compliance Team, which conducts an initial two-part evaluation: a country review and an analysis of the specific opportunity.

The country review is based on ten well-regarded governance and human rights indices, some of which include multiple sub-indices. These are the World Bank Worldwide Governance Indicators, the Economist Democracy Index, Freedom House reports, Transparency International's Corruption Perception Index, CIVICUS Civil Society Index and TRACE International Bribery Risk Matrix. These indices collectively assess factors such as human rights conditions, media freedom, rule of law, political stability, and perceived corruption within the potential customer's country. The outcome is a "Country Score" from 1 to 100, using a system that is regularly reviewed and adjusted. We are continuously evaluating the existing indices to ensure their relevance and reliability while actively exploring additional indices that may further enhance our practices.





Alongside the country assessment, the Compliance Team evaluates the specific opportunity and assigns it an "Opportunity Category" (A, B, C, or D) based on factors such as product type, customer organization and defined missions, geographical limitations, export control laws, and customer ratification of international human rights conventions.

	Opportunity category			
Country score	A	B	C	D
Above 60	Low	Low	Moderate	No engagement
46–60	Low	Moderate	Elevated	
26–45	Moderate	Moderate	Elevated	
Below 25	No engagement			

In 2024, NSO Group raised the threshold of the minimum Country Score required for new country engagement from 25 to 35.

We do not engage with customers or suppliers in sanctioned countries, those on the Financial Action Task Force (FATF) blacklist, or countries that fail to meet our human rights standards.

Based on both the Country Score and Opportunity Category, the opportunity is classified as low, moderate, elevated risk, or no engagement. Additionally, we maintain a list of "D countries", with which we will not conduct business. Currently this list includes over 60 countries. This list is reviewed and updated at least annually by our Management Committee or in reaction to major political changes.

Following the initial risk assessment and classification, the Compliance Team conducts a due diligence review. This process is tailored to the risk category assigned to the opportunity and involves gathering information from a variety of sources, including open-source research, internal discussions, interviews with potential customers, and reports from external consultants or investigative firms.

The information typically collected includes: checks for denied parties, adverse media searches (in both English and relevant local languages), a review of the domestic legal framework governing surveillance and data protection, the customer's internal processes and safeguards, reputational information related to human rights, input from relevant government bodies, and analysis of applicable export control laws and embargo lists.

Once the due diligence is complete, the Compliance Team prepares a report summarizing findings and any proposed mitigation measures. This is reviewed by the General Counsel, who may

confirm or adjust the initial risk classification based on the gathered information. If a higher risk category is warranted, the Compliance Team must conduct additional due diligence as outlined in the Human Rights Due Diligence (HRDD) Procedure.

After this process, the proposed opportunity undergoes final review by the Management Committee. For moderate- and elevated-risk opportunities, enhanced measures may be implemented to mitigate risks of misuse. These can include additional human rights training, contractual safeguards, periodic certifications, on-site audits, enhanced technological restrictions, continuous monitoring of human rights reports, and specific customer engagement mitigation measures. The Management Committee provides a report of all reviewed opportunities to the GRCC every six months. The GRCC itself can review engagements deemed to involve heightened risks, which lack unanimous approval by the Management Committee, or require further attention.

The following chart summarizes the due diligence requirements for each risk level:

	Risk/Source	Low	Moderate	Elevated
Open Source Intelligence	Results of open source adverse media search	✓		
	Report prepared by external investigative firm providing results of local language adverse media search, customer organization overview, and foreign policy and human rights-related information		Level 1	Level 2
Human Intelligence	Sales Manager questionnaire	✓	✓	✓
	Client Executive activity report [N/A for renewals]	✓	✓	✓
	Technical Support questionnaire [N/A for new End-User]		✓	✓
	Partner questionnaire	✓	✓	✓
	Advanced intelligence collected by external investigation firm		Level 1	Level 2
	Strategic input from government authorities			✓
Legal Framework	Publicly available information about local domestic legal framework		✓	
	Local legal opinion			✓
	Export controls (EU, United States, Israel)		Level 1	Level 2
	SDN/embargoed countries	Level 1	Level 2	Level 2
	End-user questionnaires/interviews			✓

3.4.2 Mitigations

The mitigation measures we implement are designed to prevent the misuse of our products, particularly in scenarios where opportunities are classified as moderate or elevated risk. These strategies align with the *U.S. Department of State's Guidance on Implementing the UN Guiding Principles for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities*, as well as international human rights standards. Our framework is comprehensive and involves a combination of proactive customer engagement, contractual safeguards, training, and continuous monitoring to mitigate potential risks.

At the core of our mitigation strategy is the requirement that every customer contract includes human rights compliance provisions.

All customer contracts include human rights provisions, with additional safeguards added based on the risk profile of the engagement. We require compliance both with domestic laws as well as international human rights standards, particularly regarding privacy, freedom of expression, and

protection against discrimination. Surveillance activities must only be conducted for legitimate purposes, i.e. combating terrorism or serious crime, and all actions must be justified under both local law and international norms. An excerpt of the human rights compliance provisions has been attached as an annex to the Company's first Transparency Report.

Technological restrictions are another key element of our approach to mitigating risks. For moderate- or elevated-risk engagements, we impose enhanced restrictions on the use of our products, such as limiting the amount of installations, geographic coverage, and the overall operational scope of the technology. These controls are designed to minimize the potential for product misuse whilst making sure that customers can still fulfill their legitimate and lawful mandates. In addition, we embed specific customer-side implementation safeguards per customer request that are designed to mitigate potential operator misuse.

In parallel, we actively monitor open-source information and public reports that may suggest human rights violations in the countries where our customers operate. Such monitoring allows us to take preemptive steps, such as requiring additional customer undertakings, imposing stricter safeguards, or suspending operations if warranted by the circumstances. In cases of heightened concern, we also engage external experts to provide an additional layer of review and ensure our response is informed by a wide range of perspectives.

Our approach to human rights compliance extends beyond contractual obligations to include a comprehensive training program. New employees receive dedicated human rights training during their onboarding, and existing staff in key functions such as presales, sales, marketing, customer executives and technical support participate in regular sessions designed to reinforce our commitment to these principles. Importantly, we also offer similar training to our customers, all in order they fully understand their responsibilities regarding the use of surveillance technologies and the protection of fundamental rights.

Furthermore, customers are required to establish grievance mechanisms through which third parties can raise concerns about human rights violations related to the use of our products. Customers are obligated to investigate any such allegations, notify us of their findings, and implement remedial actions, such as deleting improperly obtained data or retraining or dismissing personnel involved in misuse.

Finally, in engagements where domestic laws are not fully aligned with international norms, or where regulations are unclear, we require customers to develop and implement detailed and designated protocols governing the use of our products. These protocols must include criteria such as legitimate evidence supporting surveillance requests, specific crimes under investigation, data retention periods, and independent oversight approval.

Moreover, the HRDD Procedure mandates that due diligence for each customer to be renewed annually or sooner if necessary, such as when significant changes occur in the customer relationship. As part of our proactive oversight, we conduct periodic human rights compliance certifications and demand declarations from customers to confirm their adherence to legal and human rights obligations. These declarations are especially important during maintenance or contracts renewals in order to verify that our HRDD remains ongoing and up to date. Additionally, we carry out on-site audits, either through our Compliance Team or independent third-party auditors, to evaluate the implementation of these safeguards. This auditing process helps to verify the effectiveness of customer compliance and detect any potential areas of concern before they escalate.

Further details on our mitigation efforts can be found in our previous reports.

3.4.3 Reporting and Investigations

NSO Group's investigation and reporting procedures are aligned with the UNGP, encouraging both internal and external stakeholders to report concerns regarding potential product misuse. Our grievance mechanisms, established through our Internal and External Whistleblowing Policies, allow for both confidential and anonymous reporting. These mechanisms apply to employees, business partners, customers, and potentially affected individuals.

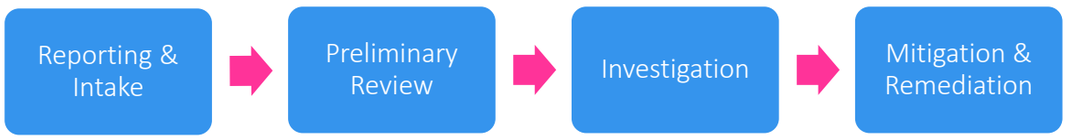
Our Internal Whistleblowing Policy, introduced in September 2019, promotes an "open door" approach, protecting whistleblowers from retaliation. Employees and internal stakeholders can report concerns directly to senior management, including the CEO, GC, and Deputy GC, or use a confidential and designated whistleblowing email account at: whistleblowing@nsogroup.com. Interaction with investigators is encouraged to ensure a thorough review of all facts.

The External Whistleblowing Policy, also adopted in 2019, allows external parties such as business partners and affected individuals to report grievances via a confidential and designated email account: at: whistleblowing@nsogroup.com. External stakeholders are assured protection against retaliation and are encouraged to engage with investigators. In cases where anonymity is preferred, communication can be facilitated through a mutually agreed third party, maintaining the whistleblower's confidentiality. In addition to formal reports, we closely monitor public reports and civil society outreach to identify potential product misuse.

36

whistleblower complaints received

Once a concern is raised, a preliminary review is conducted to determine whether there is sufficient information to warrant a full investigation. This involves identifying key details, such as the potential end-user, the alleged misuse, and the technical feasibility of the claims. If the review justifies further action, the matter is escalated to the Management Committee, which appoints a specialized investigation team. The team assesses factors such as customer adherence to legal frameworks, human rights norms, and contractual obligations. Investigations may include data reviews, interviews, and external expert consultations.



Investigation outcomes are presented to the Management Committee, and when necessary, corrective actions are taken, ranging from customer retraining to the termination of the relationship. Even in cases where misuse is inconclusive, additional mitigation measures are implemented to prevent future misuse.

Details of our product misuse investigation procedure can be found in our previous reports.

4 Product Responsibility and Human Rights

4.1 Human Rights by Design: Innovation in Safeguards and Controls

We understand the sensitive nature of surveillance technology. That is why we have built strong safeguards into our products from the ground up, focusing on responsible use and strict compliance with legal standards. Our approach ensures that every stage of our technology's development and deployment prioritizes ethical considerations, transparency, and respect for individual rights.

We are committed to preventing, to the best of our ability, potential misuse and maintaining the highest standards of accountability in a complex technological landscape.

- **"Kill switch"** – One of the foremost safeguards we employ is our "kill switch" functionality, a feature designed to immediately and remotely disable our Pegasus system in the event of unauthorized usage. The kill switch acts as a critical control point, enabling us to render the system inoperable if we detect or suspect any form of non-compliance. By activating this feature, all system capabilities are fully shut down, and Pegasus disconnects from any monitored device, effectively halting all surveillance activities. The kill switch is engineered in a manner that ensures that reactivation of the system can only occur following our explicit authorization. This approach not only supports ethical standards but also serves as a vital reassurance to stakeholders concerned with the responsible deployment of our technology.
- **Audit log of customer activities** – The Pegasus system provided to customers also includes an immutable audit log, which provides a detailed record of all activities conducted within the system which is stored on the customer's system and can be reviewed by the Company during an investigation subject to customer consent. Certain action by authorized users – such as device identifiers, operational commands, and general usage and connectivity patterns – are securely stored within such log and cannot be modified, altered or deleted. The audit log serves as a foundational component of our oversight and accountability practices, enabling us to conduct investigations and verify compliance with established guidelines. In cases where potential misuse is suspected, the audit log allows for a transparent and documented review process with the cooperation of the customer.
- **Compartmentalized research structure** – NSO Group has also implemented strict controls on the research, discovery, and management of system vulnerabilities. Our approach limits access to and knowledge of discovered vulnerabilities, operating under a compartmentalized research structure where each researcher is responsible only for their specific area. Only a small, vetted team within the Company has a comprehensive understanding of the full vulnerabilities chain, thus ensuring operational security by minimizing any risks associated with unauthorized access or disclosure of vulnerabilities.
- **Limited customer access** – Vulnerabilities, once identified, are securely integrated into Pegasus under a "black box" framework. This means that customers are not granted direct access to vulnerabilities or individual components of the system; rather, the vulnerabilities are embedded in a manner that limits user interaction solely to approved functions of the technology. Researchers at NSO Group operate under stringent non-disclosure agreements (NDAs) and other contractual obligations, prohibiting any independent sale, sharing, or engagement with vulnerabilities.
- **Blocking unauthorized transfer** – Preventing unauthorized transfer of our products by customers is another core element of our human rights compliance strategy. We take a multi-layered approach to prohibit customers from engaging in onward transfers, addressing the serious risks posed by unauthorized distribution. Each installation of our products is restricted to customer on-premises infrastructure, and access points are tightly monitored and controlled. We have in place an authentication system that verifies each device and user through their IP, making any unauthorized connection impossible. That means that if the system is attempted to be moved or used on unauthorized hardware it automatically becomes inoperable, thanks to our product's security protocols that tie it specifically to preapproved devices and network configurations.

In addition to the technological security protocols, we comply with export control policies, as our technologies are classified as “defense articles” and are sold exclusively to vetted government agencies. Each customer is required to sign an end-user certificate, a formal Government-to-Government commitment that strictly prohibits onward transfer or unauthorized use of our products. Violations of this agreement not only breach the terms of use but also violates international legal standards, incurring potential significant legal and diplomatic consequences.

These terms are incorporated in our customer contracts, which also include explicit prohibitions against unauthorized transfers, backed by legal penalties such as termination of service. To further enforce these agreements, we conduct regular due diligence and verification procedures as described in length in this report. On-site compliance audits also support our risk management efforts, allowing us to verify that customers’ system usage remains in line with NSO’s contractual and regulatory commitments.

Moreover, NSO Group has implemented a set of mechanisms for customers use only in order for them to verify target identification and prevent unauthorized access by their personnel. These include safeguards to block surveillance on identifiers – unique markers such as phone numbers or device IDs that distinguish specific individuals – that appear on a predefined restricted list, ensuring such individuals cannot be targeted. Additionally, the system incorporates an operator statement protocol requiring users to confirm that each installation request complies with applicable legal standards and is authorized under relevant laws These safeguards are complemented by warrant management functions, which allow the customer’s operators to specify warrant requirements on a case-by-case basis, thus making sure all installations are backed by appropriate legal documentation.

Over 10%

compliance-related expenditure out of the total

Rights We Seek to Protect

- **Right to Life,** Universal Declaration of Human Rights (“UDHR”) Article 3; International Covenant on Civil and Political Rights (“ICCPR”) Article 6
- **Right to Liberty and Security,** UDHR Article 3; ICCPR Article 9
- **Right Not to Be Held in Slavery or Servitude,** UDHR Article 4; ICCPR Article 8
- **Right Not to Be Subjected to Torture or to Cruel, Inhuman, or Degrading Treatment or Punishment,** UDHR Article 5; ICCPR Article 7
- **Right Not to Be Subjected to Arbitrary Arrest or Detention,** UDHR Article 9; ICCPR Article 9
- **Right to Liberty of Movement and Freedom to Choose Residence,** UDHR Article 13; ICCPR Article 12

4.2 Future of Responsible Technology Development

When thinking on the future of responsible technology development, we are exploring a range of safeguards and controls that we believe could set an ethical and operational standard across the industry. While some of these features are in various stages of development, and some are already in place or in implementation phase, each is designed to contribute to a framework for responsible technology use and ultimately support the broader objective of mitigating potential misuse.

Collectively, these controls reflect a human rights approach for embedding accountability and oversight into the very architecture of surveillance technologies, aiming to protect vulnerable groups and sensitive targets without the need for direct, ongoing access to operational information, which obviously cannot be granted.

The proposed controls and safeguards for the industry originated from a synthesis of insights across multiple disciplines each offering valuable perspectives on ethical technology development, such as privacy, data protection and IT. These safeguards are also recognized within international human rights guidelines, including the UNPGs, and reflect industry best practices and ethical considerations that are essential for any responsible deployment of surveillance technology. Moreover, the academic literature on surveillance ethics and human rights advocates for implementing these types of controls to balance security objectives with fundamental rights.

- **Built-in warrant management system –** This system embeds legal authorization requirements directly into the surveillance product's functionality, ensuring no surveillance actions are taken without prior, verified legal approval. By integrating this step into the operation workflow, organizations could automate compliance with legal standards, requiring operators to provide appropriate documentation and credentials before surveillance activities proceed and access only the approved data within the approved time specified in the warrant. This approach minimizes risks of unauthorized use, as the system itself enforces the initial legal authorization check. At scale, a warrant management system could standardize legal compliance across various jurisdictions, making it easier for organizations to manage regulatory obligations and confirm lawful access.
- **Measures preventing unauthorized transfer of surveillance products –** Focus on ensuring that each installation is restricted to customer infrastructure, with controlled access points authenticated by the provider. Any attempt to relocate the system or access it through unauthorized devices renders the technology inoperable, helping to prevent its misuse and maintain secure, on-premises operations.
- **Non-bypassable configurations and system restrictions** – Ensure that surveillance tools adhere to contractual and ethical standards set for each customer. By embedding configurations inaccessible to the user in secure areas, these products remain within the functional boundaries approved by the technology provider.
- **Target verification and operator statements** – These controls are intended to ensure lawful, documented surveillance requests. A target verification process blocks predefined identifiers that have been flagged, while operator statements require a declaration affirming the legality of each surveillance operation. This feature, when combined with warrant management systems, creates an additional layer of transparency and legal adherence, fostering responsible use at each operational level.
- **Predefined safeguards for sensitive operations** – By implementing settings that prevent or delay certain types of surveillance actions until additional approvals are obtained, predefined safeguards add another layer of ethical control. These settings could be customizable, allowing organizations to configure restrictions according to internal governance, specific operational risks, or identifying sensitive groups. For instance, surveillance targeting specific sectors, individuals, or locations could be flagged, and the system would require a separate level of verification before proceeding. These safeguards would serve as an automated reminder to adhere to agreed-upon ethical standards, creating a framework for careful consideration before high-risk activities are initiated. This feature would further contribute to accountability, allowing organizations to demonstrate due diligence and ethical sensitivity in their operations.
- **Role-based access control (RBAC)** – RBAC would limit system access based on each operator's role, expertise, and level of clearance, with sensitive system capabilities restricted to authorized and qualified personnel. This segmentation ensures that only those with appropriate training and experience can initiate or oversee surveillance activities, adding a vital layer of oversight. Through a hierarchy of access levels, the RBAC system would control access based on the task's sensitivity and the operator's authority. In terms of protecting vulnerable populations, RBAC prevents lower-level of untrained operators accessing or conducting sensitive surveillance tasks, reducing misuse risks.

- **Enhanced usage logs and reporting** – Enhanced logging functionality records details of all system activities, including who accessed the system, what surveillance actions were initiated, and what approvals were obtained. These logs would be immutable, preventing alteration, deletion, or tampering by operators. The level of detail within these logs could be customized to meet oversight requirements, including periodic reports that can be reviewed internally or by third-party auditors. By maintaining a clear, verifiable record of activities, organizations can respond transparently to concerns about system use, while independent reviews could add further layers of accountability. For sensitive populations, enhanced logs offer a tangible way to review and verify that all activities comply with regulatory and ethical standards.
- **Real-time monitoring alerts** – This feature would send instant alerts to customer compliance teams or designated customer governmental third parties when certain high-risk actions or sensitive operations are initiated. By proactively flagging specific system actions or target types, the alerts create a continuous layer of monitoring. This function does not disclose detailed operational information, maintaining user confidentiality while notifying oversight parties of potentially concerning actions. For example, if a surveillance request matches parameter associated with a protected demographic, an alert could trigger immediate review by functionaries designated by the customer, providing an additional safeguard without compromising operational privacy.
- **Adaptive risk scoring and multi-level approvals** – Adaptive risk scoring would evaluate the risk level associated with each surveillance request in real-time based on predefined factors, such as operator identity, target type, location, or specific operational conditions. Higher risk scores could automatically require multi-level approvals, necessitating review by customer senior personnel or an ethics committee before the request can proceed. This scoring mechanism introduces a dynamic assessment into the workflow, providing safeguards that respond adaptively to evolving contexts. When combined with multi-level approvals, this feature offers an escalation pathway which ensures that only high-ranking, accountable parties approve sensitive actions, reducing the likelihood of unverified access or unauthorized surveillance.
- **Anomaly detection** – Anomaly detection would monitor for unusual behavior patterns within the system, such as unexpected access times, irregular request volumes, or any deviations from established usage norms. This feature could flag potential misuse or unauthorized access in real-time, providing internal compliance teams an opportunity to investigate and halt questionable activities. Anomaly detection is particularly valuable in identifying insider threats or addressing improper behavior before it escalates. Through this functionality, organizations can maintain a proactive stance on potential misuse, further reinforcing ethical standards without compromising operational confidentiality.
- **Embedded compliance training** – This feature would integrate ongoing ethical and legal training directly into the system, keeping operators current on regulatory obligations and ethical guidelines. For instance, each time an operator accesses the system or initiates a specific task, compliance reminders or training modules could be automatically displayed to reinforce the importance of ethical surveillance practices. This embedded training keeps responsible practices top of mind for operators, reinforcing compliance with both legal and organizational standards. The direct, accessible format can promote a culture of accountability and prevent unintentional policy violations by ensuring operators understand the full ethical scope of their work.
- **On-demand compliance audits** – This feature would allow organizations to perform real-time compliance audits, providing an accurate snapshot of system use at any given moment. Audits could be conducted internally or by a third party, assessing usage patterns, adherence to guidelines, and alignment with ethical standards. An on-demand audit capability adds flexibility, enabling organizations to respond quickly to emerging concerns or specific requests.

NSO Group has developed versions of several measures outlined here, including warrant management systems, and enhanced usage logs. These features are primarily designed for customer-side implementation, because vendors, like NSO Group, are not privy to or aware of which controls are activated. All controls could be embedded in the product per customer's request in order to meet domestic legal or regulatory requirements or organizational internal operational guidelines. The Company is actively evaluating the development and implementation of additional safeguards within our products to even further mitigate the risk of misuse. These safeguards will be designed to address new and emerging risks in our field. New substantial and

material safeguards that are developed and implemented will be reported in our next Transparency Report.

In addition, it is important to recognize that not all safeguards are universally applicable or customized to every technological tool and can also vary based on end-user organization type. There is no "one-size-fits-all" approach in this dynamic field. However, we believe that the controls and safeguards outlined here may contribute significantly to the broader goal of keeping these powerful technologies aligned with ethical practices and respect for human rights.

Furthermore, these safeguards are designed with the confidentiality and secrecy essential to our customers' sensitive work in mind. With these safeguards, private technology providers continue to remain separate from the specific details of intelligence and law enforcement activities and do not have any access to or visibility into customer operations. This approach allows customers to conduct their operations with full operational security and ensures that intelligence and law enforcement agencies maintain full control over their sensitive work.

This separation means that intelligence or law enforcement activities remain fully shielded from the technology provider, ensuring no sensitive information or details about customer operations are accessible, even as safeguards work to prevent misuse and promote ethical standards.

5 Access to Remedy

5.1 Methodology for Product Misuse Investigations

At NSO Group, we have implemented an investigative process focused on potential misuse of our technology. This process guides us in handling concerns that a customer may have misused our products

- **Reporting channels for internal and external stakeholders** – Our investigation process starts by making it easy and safe for people to share their concerns. Reporting channels are open to anyone involved with our products, from employees and partners to customers and affected individuals. These channels, governed by our **Internal and External Whistleblowing Policies**, maintain confidentiality and encourage transparency. We also allow for anonymous reporting, so that individuals can choose to reach out directly to management, use a dedicated confidential email, or speak through secure, third-party intermediaries. This flexibility helps ensure everyone feels safe when reporting concerns.
- **Intake and preliminary review –** After receiving a report, we conduct a preliminary review to evaluate whether the Company has sufficient information regarding an alleged misuse that would necessitate a formal investigation under NSO's procedure. This initial check includes looking into the basic details: understanding who reported, identifying the alleged end-user, and evaluating the type of alleged misuse and if it aligns with the technical capabilities of our product. This step can filter out baseless or incomplete claims and allows us to focus on cases that genuinely need further review, helping us utilize resources effectively.
- **Management committee review and investigation authorization –** Reports with credible allegations are escalated to the Management Committee, which decides on authorizing an in-depth investigation. The committee reviews initial findings, weighing legal and ethical considerations. Based on the Committee evaluation, they decide whether to move forward with a full investigation. If approved, they assign a specialized team, potentially with outside experts, to ensure the process remains objective and in line with legal and human rights standards.
- **Comprehensive fact-finding and data analysis** – The investigation team conducts a comprehensive fact-finding phase, which includes analyzing case data, usage patterns, relevant logs, and additional open-source intelligence (OSINT) and human intelligence (HUMINT) sources. When necessary, interviews with involved stakeholders help gather further context. Independent experts, including legal and human rights advisors, contribute perspectives, comprehensive analysis aligned with our human rights and compliance standards.
- **Investigation process** – Our investigation steps aim to carefully examine the details and reach balanced conclusions:
    - **Preliminary data gathering** – First, the team gathers available reports, data, and information about local legal safeguards on privacy and surveillance.
    - **Review of customer activities** – When needed, the compliance team organizes a meeting with the end-user to understand the context of any alleged misuse. This involves preparing by gathering relevant information from local experts or other sources and setting up an in-person interview, ideally at the end-user's site. During this interview, the Company's representatives review the end-user's compliance with contractual terms and local laws, including any processes for protecting individual rights and due process. Topics include the end-user's mission, investigative processes, types of cases where the Company's products are used, and details about any human rights concerns or past allegations. The interview then delves into the details of the specific case that is being investigated to understand the process that was actually implemented in the specific case and its compliance with legal, contractual and ethical requirements. The discussion also covers how the information gathered was used in practice – whether for evidence in a case or crime prevention only.

- **Review of audit logs** – In cases where the customer denies allegations of misuse, we review audit logs to verify system usage and assess compliance with contractual and legal obligations.

- **Supplemental actions** – Where necessary, additional measures, such as temporary system restrictions or the consultation of external experts, will be implemented.
- **Legal framework analysis** – We usually will conduct a legal review, often with local counsel's help, to ensure the customer's actions are lawful and that proper privacy safeguards are in place.

Failure of an End User to cooperate in this process may lead to immediate termination of the relationship with this customer.

- **Assessment against compliance and human rights standards** – Next, the investigation team evaluates findings against the customer's contractual representations and undertakings and other human rights standards, ensuring the customer's actions align with our contractual provisions and international human rights norms.
- **Presentation of findings and decision-making –** The investigation findings together with recommendation of remedial action are presented to the Management Committee, which decides on an appropriate course of action following the investigating team recommendations. In cases where misuse is substantiated, possible actions may include retraining, pre-certification, or even suspending or terminating the customer relationship. Inconclusive cases may still prompt us to implement additional safeguards to mitigate future risks.
- **Post-investigation follow-up and continued oversight –** Following each investigation, we monitor customer activity to ensure ongoing compliance with any corrective actions taken. Additional training sessions may reinforce best practices, and insights from each case contribute to refining our compliance standards, supporting continuous improvement.
- **Documentation, transparency, and accountability –** Our team documents each investigation phase, including findings, corrective measures, and final determinations. This documentation allows us to report transparently and audit our processes. When appropriate, we also share aggregated insights from our investigations with stakeholders to demonstrate our commitment to ethical practices and respect for human rights.

5.2 Product Misuse Investigation Case Studies

Disclaimer: All identifiers in the following case studies, including individuals, countries, and organizations, have been anonymized to maintain confidentiality in accordance with legal, regulatory and contractual obligations.

5.2.1 Case Study 1: Investigation Resulting in Termination

Incident overview

NSO Group received credible reports alleging that individuals belonging to a protected community had been targeted using its technology by one of its customers. The customer, a government entity, was identified through an internal inquiry as the likely source of the alleged misuse.

Customer interaction

NSO Group immediately engaged with the customer to investigate the claims. A formal meeting was held, and detailed questionnaires were submitted to the customer seeking clarification on the following:

- The basis for targeting each individual, including whether they had threatened or committed violent acts against citizens
- Whether legal authorizations or warrants had been obtained for surveillance, including details on the approval process
- Evidence of alleged crimes committed or threats to national security or regime stability
- Specific examples and dates justifying the surveillance activities
- General questions regarding the customer's legal framework for surveillance and its alignment with NSO Group's contractual obligations and human rights standards

In response, the customer claimed that the individuals in question were suspected of disseminating material that, in their view, incited violence and posed a security threat.

Independent review
NSO Group thoroughly examined the customer's responses, including the evidence provided, to determine whether the targeting met the threshold for legitimate surveillance under the Company's guidelines and human rights commitments. After careful analysis, we found the justifications provided by the customer to be insufficient and unconvincing. There was no clear evidence demonstrating that the individuals had engaged in unlawful activities or posed a legitimate security threat that would warrant surveillance.

Findings
The investigation concluded that the customer's actions constituted a material breach of NSO Group's contractual obligations and human rights standards, and was inconsistent with both NSO's guidelines and international human rights norms.

Outcome

As a result of the findings, NSO Group issued a termination notice to the customer. The notice outlined the material breach and declared that:

- The agreement with the customer was deemed terminated
- All licenses and services were canceled
- The customer's access to NSO's technology was permanently revoked

5.2.2 Case Study 2: Investigating Alleged Misuse and Implementing Alternative Remediation

Incident overview

In 2023, NSO Group received a media inquiry alleging that an individual, identified as a public advocate working abroad, had their communication device compromised using Pegasus technology. Based on the information provided, NSO Group identified one of its customers – a country recognized globally for its strong human rights record and adherence to international legal norms – as the likely entity associated with this claim. The customer operates under rigorous national security protocols and maintains a high standard of governance.

Customer interaction
NSO Group immediately engaged with the customer to address the allegations. The customer, citing national security restrictions, was unable to provide specific details regarding the alleged incident but confirmed that all operations involving NSO technology are conducted within the boundaries of local laws and contractual obligations.

The customer explained that their surveillance activities are closely tied to safeguarding national security and countering potential threats – these statements were enforced by the customer's legal department which also approved and verified the legality of the surveillance operations after conducting their independent internal audit. External independent OSINT reports highlighted past

instances where individuals posing as professionals in trusted fields were discovered to have links to adversarial activities.

Independent review
To ensure a thorough investigation, NSO Group commissioned 2 independent reviews:

1. **Enhanced research and due diligence** – A detailed assessment of open-source information and discreet inquiries were conducted to evaluate the legitimacy of the individual and their activities. Open-source report did not include specific information that was relevant to this incident.
2. **Legal framework assessment** – A comprehensive review of the customer's legal and regulatory environment was performed by an independent domestic legal expert. The analysis confirmed the presence of robust oversight mechanisms, including requirements for independent judicial approvals, proportionality assessments, and strong due process safeguards.

Findings

The independent reviews supported the conclusion that the customer's use of the technology complied with local laws and contractual requirements.

Key findings include:

The legal review reaffirmed that the customer's surveillance framework adheres to international human rights norms, emphasizing independent oversight and due process

Mitigating measures

In light of these findings, NSO Group implemented alternative remediation measures to strengthen compliance and prevent potential misuse in the future:

- Confirm **enhanced human rights provisions in end-user agreement**.
- **Provide in-person human rights and permitted use training** to end-user, which shall be conducted on the end-user's premises by the Company's Compliance team.
- Periodically **review open source information about human rights conditions in the customer's country**.
- **Agree-upon monitoring activities**, such as an annual in-person meeting with the Company's Compliance Team or an agreed independent third party, which shall include the review of customer's adherence to applicable laws and Company's contractual requirements, including that: (1) The Company's products are **used only to investigate crimes covered by relevant laws** and as agreed in the NSO-end-user contract; (2) Individuals are **not being targeted for expressing dissident views or engaging in protected activities** under international human rights norms; and (3) and Surveillance **requests are reviewed and approved** by applicable, independent authorities and only with reasonable evidence to support the necessity and proportionality of the use of the Company's products on targeted individuals.
- **Obtain additional information from end-user** regarding how, in practice, requests for surveillance are submitted to and reviewed by the relevant approver, along with practices related to ongoing supervision of surveillance activities to allow NSO to confirm at a high-level that the customer is following domestic law as described by local counsel.

5.3 Real-Time Product Misuse Investigation Reporting Dashboard

NSO Group is evaluating introducing a Real-Time Product Misuse Investigation Reporting Dashboard to provide greater transparency in how we handle product misuse investigations. The dashboard will present aggregated data on the investigation process.

In order to maintain the integrity of this approach, the data will be aggregated and will be refreshed quarterly to avoid any association with specific outreach, reports, or alerts, to the

commencement of an investigation as we cannot confirm nor deny the existence of any customer in a particular country. This approach follows industry standards and ensures that we remain in compliance with our contractual and regulatory obligations governing our activities.

6 Measuring Effectiveness: Beyond Compliance

6.1 UNGP Compliance Survey

During the reporting period, NSO Group conducted a self-assessment survey to evaluate its alignment with the UNGPs. The survey, designed and executed by internal compliance counsel, followed the methodology outlined in the UNGP Reporting Framework, utilizing its Implementation and Assurance Guidance. The survey's methodology, key findings, and an action plan for continuous improvement were presented to the GRC Committee for review.

The survey aims to provide us with an in-depth understanding of our adherence to human rights standards, evaluating the integration of these principles into the Company's operational framework and decision-making processes.

6.1.1 Survey Methodology

The survey methodology was grounded in the UNGP Reporting Framework, a recognized structure that facilitates a thorough assessment of corporate human rights practices. The methodology comprises four key components:

1. **Policy commitment**: This aspect of the survey evaluated the extent to which NSO Group has established policies that align with the UNGPs. The assessment focused on the clarity and comprehensiveness of the Company's human rights commitments, including the integration of these policies across various levels of the organization. Evaluating this commitment provides insight into NSO Group's proactive stance in promoting human rights and ensuring that these principles are embedded in its culture.

2. **Salient human rights issues and due diligence**: This component involves identifying and assessing the most significant human rights risks associated with NSO Group's activities. The survey evaluated the effectiveness of the Company's due diligence processes, emphasizing the systematic approach to identifying, mitigating, and addressing potential and actual impacts on human rights. It was essential to assess how well NSO Group integrates the findings of these assessments into its strategic planning and operational practices, thereby demonstrating its commitment to risk management in relation to human rights.

3. **Management of salient human rights issues**: The survey examined the measures implemented by NSO Group to manage and mitigate the identified salient human rights issues. This included evaluating the integration of human rights considerations into the Company's business operations and decision-making processes. A comprehensive review of management practices revealed how NSO Group prioritizes human rights in its operational framework, ensuring that risk mitigation strategies are in place and effectively communicated across departments.

4. **Remedies and grievance mechanisms**: Finally, the survey assessed NSO Group's mechanisms for providing remedies to individuals or communities adversely affected by its operations. This included a review of the effectiveness of existing grievance channels, evaluating their accessibility, responsiveness, and the overall effectiveness in addressing human rights concerns. The assessment focused on whether these mechanisms were well-publicized and whether stakeholders were aware of the channels available for raising complaints.

6.1.2 Company Performance

The survey yielded several notable findings regarding NSO Group's performance in relation to human rights compliance. The Company demonstrated exemplary performance across various indicators, showcasing a strong alignment with both the letter and spirit of the UNGPs. Specifically, NSO Group's commitment to upholding human rights was evident through its well-established policies, robust due diligence processes, and accessible grievance mechanisms.

Despite these strengths, the survey highlighted areas with opportunities for improvement. One of the primary concerns is the **effectiveness of remedies for human rights complaints**. The limited visibility into the customer use of products and the inherent challenges in establishing direct

cause-and-effect relationships hinder the ability to fully evaluate the effectiveness of remedies. Additionally, **the tracking and progression of efforts** in addressing salient issues were constrained by contractual confidentiality and legal restrictions, making it difficult to provide concrete evidence of progress in practice. The survey also noted **gaps in stakeholder communication**, suggesting that not all relevant parties, including employees, contractors, and partners, were adequately informed and engaged regarding NSO Group's commitment to human rights.

6.1.3 Action Plan for Continuous Enhancement

In light of the findings, NSO Group has developed a targeted action plan aimed at enhancing its compliance framework and addressing identified areas for improvement:

1. **Contractual review**: The Company will conduct a thorough review of its contractual obligations with customers, seeking opportunities to renegotiate terms that would allow for greater transparency in evaluating the effectiveness of mitigations and remedies, without compromising full separation from customer's operation.

2. **Enhanced tracking and reporting**: The Company aims to develop and implement a comprehensive framework for systematically tracking and reporting on the progression of efforts in addressing salient human rights issues. This framework will integrate qualitative and quantitative indicators to better demonstrate impact over time.

3. **Stakeholder communication and engagement**: The Company recognizes the need to strengthen its communication channels and engagement strategies. The company is committed to ensuring that all stakeholders are effectively informed about its human rights commitments and practices.

4. **Ongoing monitoring and policy adaptation**: Continuous monitoring and periodic updates to policies will be implemented to align with evolving human rights standards and best practices. This adaptive approach will ensure that the Company human rights frameworks remain responsive to changing dynamics in the industry.

The Company will be providing an update on the progress of the action plan. This update will be included in our next Transparency Report, where we will outline the steps taken, any challenges faced, and the actions the Company implemented to further align with the UNGPs.

6.2 Human Rights Scores of Customers

6.2.1 Methodology

The evaluation of human rights performance for prospective and current customers is a core element of the Company's human rights compliance framework and is an essential part of our initial assessment of customers' risk exposure. To ensure a thorough and objective assessment, the Company assigns a human rights score to each customer country.

The score is calculated through a comprehensive review of the customer country's governance, human rights, and rule-of-law record, practices and frameworks, using credible external indices and internal scoring criteria. A "Country Score" ranging from 1 to 100 is determined, with higher scores reflecting stronger governance, human rights protections, and institutional safeguards. The methodology prioritizes three primary dimensions:

- **Freedom of speech and incorporation of human rights and civil liberties:** Weighted at 50%, this evaluates the extent to which freedoms and rights are upheld.
- **Rule of law and political stability:** Weighted at 40%, this assesses the governance framework's ability to maintain democratic norms and stability.
- **Corruption:** Weighted at 10%, this examines transparency and the presence of systemic corruption, as these factors significantly influence governance quality and human rights protections.

The Compliance Team annually reviews the scoring methodology to ensure it remains up-to-date, and adaptive to evolving global standards and emerging risks.

6.2.2 Analysis of External Indices Used

NSO Group relies on data from ten highly regarded and readily-available open source governance and human rights indices to inform its GRC scoring system. These indices provide a multidimensional view of each country's human rights environment and governance structures:

- **World Bank Worldwide Governance Indicators:** Analyzes governance quality, including rule of law, government effectiveness, and corruption control.
- **Economist Democracy Index:** Measures the health of democracies, focusing on electoral processes, civil liberties, and political culture.
- **Fund for Peace Fragile State Index:** Highlights vulnerabilities in governance, social cohesion, and human rights that contribute to state fragility.
- **Freedom House Freedom in the World Report:** Assesses political rights and civil liberties, providing a snapshot of freedom and democracy.
- **Freedom House Freedom on the Net Report:** Evaluates digital rights, including censorship, online freedoms, and access to information.
- **Reporters Without Borders Freedom of Press Index:** Measures media independence and freedom of expression, key indicators of civil liberties.
- **Transparency International Corruption Perceptions Index:** Ranks countries based on perceived corruption levels, an essential governance metric.
- **Global Peace Index (GPI):** Evaluates societal safety and security, as well as conflict levels, reflecting stability and governance quality.
- **CIVICUS Civil Society Index:** Assesses the environment for civil society organizations, including freedom of association and public participation.
- **TRACE International Bribery Risk Matrix:** Evaluates bribery risks and business integrity, critical for ethical governance assessments.

By evaluating and analyzing these indices, NSO Group ensures that its human rights scoring framework integrates credible, diverse, and globally respected data sources for comprehensive country assessments.

6.2.3 Trend Analysis: Improving Customer Country Scores

The 2024 analysis of NSO Group's customer portfolio highlights significant improvements in the human rights conditions of its customer countries, underscoring the impact of the Company's enhanced compliance program. Key findings include:

1. **Improved country scores across the portfolio:** Since 2018, the average human rights score of NSO Group's customers has steadily increased. This indicates the effectiveness of the Company's due diligence processes in prioritizing partnerships with governments that demonstrate a commitment to human rights and democratic principles.
2. **Lower-risk customers:** Approximately 85% of NSO Group's current customers are classified as low- or medium-risk. These customers operate in countries with robust human rights protections, strong rule-of-law systems, and effective governance mechanisms. Over the past years, we have observed a steady and significant reduction in the percentage of high-risk customers in our portfolio. This positive trend is a direct result of the Company's rigorous vetting procedures, which have been strengthened to ensure that we partner only with customers who demonstrate a commitment to ethical standards, responsible governance, and the legitimate use of our technologies.
3. **Alignment between risk classification and technology allocation:** The analysis revealed a deliberate allocation of technological capabilities based on customer risk levels: Low-risk customers are granted access to more sophisticated and intrusive tools, reflecting their adherence to high human rights and governance standards and robust institutional safeguards, while high-risk customers are limited to less intrusive technologies, reducing potential human rights risks in cases of misuse.

6.3 Validation of Enhanced Compliance Measures

The continuous improvement in customer country scores and findings from the UNGP compliance survey self-evaluation validate NSO Group's focus on responsible practices. These assessments underscore the Company's progress in advancing human rights due diligence and promoting ethical practices in the industry.

7 Human Rights in Value Chain

As mentioned previously in this report, managing suppliers in the cyber intelligence industry is critical, not just for operational success but also for upholding ethical and human rights standards. Suppliers, such as independent researchers offering vulnerabilities or exploits but virtually all kinds of suppliers and vendors, play a key role in the value chain, but working with them requires careful vetting to ensure trust and accountability. This process involves verifying their identity, assessing their reputation and motivations, and ensuring alignment with ethical practices. By prioritizing rigorous supplier management, companies can reduce risks and demonstrating their commitment to responsible business practices. This is especially important in a sector where the misuse of technology can have profound adverse impact and consequences on human rights.

7.1 Supplier Code of Conduct

Our Supplier Code of Conduct shows how we put human rights into practice across our entire supply chain. Built on international standards like the UN Universal Declaration of Human Rights, the code sets clear expectations for every company we work with. It represents a core part of our business strategy, making sure that our commitment to ethical practices extends beyond our own operations.

We see our suppliers as partners, not just vendors. When they work with us, they commit to maintaining high ethical standards – not only in their own operations but also with their own suppliers. This creates a chain reaction of responsible business practices that extends far beyond our direct relationships. The code's requirements encompass human rights, labor standards, environmental responsibility, and business ethics, creating a comprehensive framework for sustainable business operations.

This approach reflects a simple truth: our success as a business is linked to how responsibly we and our partners operate.

By choosing suppliers who share our commitment to ethical practices, we are building stronger, more sustainable business relationships that benefit all parties involved. Through our Supplier Code of Conduct, we are fostering a business ecosystem where ethical conduct and commercial success go hand in hand.

7.2 Supplier Due Diligence

We conduct due diligence on all our business partners and material suppliers through a risk management platform. This system enables us to perform automated risk assessments across our entire third-party network, screening for key risk categories including anti-corruption, human rights, and environmental factors. The platform consolidates information from global sources, providing us with detailed insights through weighted risk scores. Our screening process includes sanctions checks of all third parties and adverse media monitoring, litigation findings and political exposure assessment when warranted based on our risk assessment, thus ensuring that we maintain a complete understanding of our business relationships. We carefully evaluate all third-party partners through this process. This includes checking their business practices, financial health, and reputation, with particular attention to anti-corruption compliance.

In our work with cyber vulnerability research, we set particularly high standards. We built long-term relationships with trusted vendors who share our commitment to responsible business practices. These established partnerships help us maintain consistent ethical and security standards. These relationships have allowed us to develop deep mutual understanding and trust, which is crucial in our field.

Our due diligence also includes regularly assessing our vendors, maintaining detailed records of all transactions, and making sure that we comply with international trade regulations. This ongoing monitoring includes robust "Know Your Customer" and "Know Your Transaction" procedures, supported by comprehensive documentation and regular staff training.

8 Global Dialogue: Stakeholder Engagement and Transparency Initiatives

8.1 Multi-stakeholder Forums and Working Groups

Over the past year, we have actively engaged with initiatives that bring together diverse voices to address the challenges of using advanced technologies responsibly. One such effort is the Pall Mall Process,[2] where we provided detailed input about the safeguards and controls that define our human rights compliance program, how we manage suppliers, research vulnerabilities, and what we consider as general good practices in the industry. Our contributions focused on critical areas like responsible behavior, managing risks in technology use, supplier oversight, and ensuring that customers act ethically and responsibly when utilizing our products in their operations. The draft report of Pall Mall that we have seen drew heavily on our practices, especially in the area of customer oversight, incorporating our approach as a key recommendation. This recognition underscores the strength of our compliance framework and its potential to guide the industry toward higher standards.

But our work does not stop there. We intend to expand our efforts to connect with a wide range of stakeholders – academics, think tanks, and research organizations in the U.S. and Europe – who focus on national security, intelligence, law enforcement, arms control, digital surveillance, and other related issues. By working with these groups, we aim to share our experiences, learn from experience of others and help shape public policy, discourse and governance frameworks that balance the need for security with the protection of fundamental rights and to promote a richer understanding of the complex intersection between technology, security and human rights.

These collaborations are about more than contributing to research and academia. They are about driving real change. By partnering with experts and thought leaders, we hope to advance practical, evidence-based solutions that address the ethical complexities of this industry. Our insights, drawn from operating at the forefront of these technologies, can help policymakers and researchers design regulations that are both effective and grounded in reality and, as always, we are open to receiving critique and feedback from thought leaders.

We are also intending to extend our outreach to organizations that represent the interests of law enforcement professionals, public prosecutors, and attorneys. These NGOs advocate for the use of advanced technological tools to enhance the efficiency and effectiveness of law enforcement and prosecutorial work. By engaging with these groups, we aim to contribute to discussions on how technology can support legal systems in addressing modern challenges while ensuring that its application aligns with human rights and ethical considerations. These collaborations allow us to learn from practitioners and demonstrate how our innovations can be responsibly integrated into their vital work. Additionally, we also made it a priority to engage with organizations advocating for victims of crime and vulnerable communities. These include NGOs focused on combating modern slavery, child exploitation, and human trafficking. By working together, we aim to ensure that our tools are used to protect those most at risk and to contribute to broader societal goals of safety and justice.

The impact we hope to create through these efforts is significant. We want to demonstrate that robust compliance and ethical safeguards are not only achievable but necessary for our industry.

We aim to bridge the gap between those who design and use technology and those shaping the rules that govern it.

Looking ahead, we plan to actively participate in more public policy discussions, support cutting-edge research, and contribute to initiatives that set new ethical benchmarks for the industry.

[2] The Pall Mall Process, The Pall Mall Process: Tackling the Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities (6 Feb., 2024), https://assets.publishing.service.gov.uk/media/65c25bb23f6aea0013c1551a/The_Pall_Mall_Process_tackling_the_proliferation_and_irresponsible_use_of_commercial_cyber_intrusion_capabilities.pdf.

8.2 Policy Advocacy and Industry Standards

The challenges posed by the misuse and uncontrolled proliferation of cyber intelligence tools highlight the urgent need for a unified, comprehensive and global approach to regulation. As of now, regulation varies significantly across countries, creating a patchwork of laws that often leave gaps. Some countries adopt weaker rules to prioritize their own surveillance goals or to build their own cyber intelligence industries. This lack of consistency creates confusion, making it harder to distinguish between responsible and irresponsible uses of these technologies and increasing the risk of misuse.

Therefore, we continue to advocate for a robust international regulatory framework to govern the use of cyber intelligence technologies, and our engagement with global stakeholders, as described in length in this report, reflects our commitment to this cause. Below are some key solutions we support for improving the regulation of cyber intelligence technology:

- **Establishment of a global governance body and international regulatory framework**: Create a global body to define legitimate versus illegitimate use and users, set thresholds for purchasing cyber intelligence tools, and establish universal enforcement mechanisms.
- **International licensing regime**: Establish a licensing system for the sale and transfer of cyber intelligence technologies, encouraging countries to implement such in order to ensure that only legitimate actors with human rights standards are authorized to acquire these tools.
- **Universal certification program for companies**: Develop a certification program based on adherence to international standards, human rights due diligence, and best business practices. Only certified companies would be allowed to participate in the market.
- **Independent audit mechanisms for end-users**: Introduce independent audits to verify end-user compliance with legal and contractual obligations, enabling early detection of potential misuse.
- **Global incident reporting system and grievance mechanisms**: Establish a system to track reported misuse of cyber intelligence tools, along with global grievance mechanisms for victims to raise concerns with an international body capable of investigating and providing remedies.
- **Harmonization of national legislation**: Ensure national legislation aligns with international frameworks to prevent regulatory arbitrage and discourage weak regulatory environments.
- **Promoting collaboration between industry and civil society**: Foster greater cooperation between technology companies and civil society organizations to ensure responsible use of cyber intelligence tools.

9 Looking Ahead: Future Commitments and Goals

As we look toward the upcoming year, we remain steadfast in our commitment to advancing human rights, promoting responsible technology use, and enhancing transparency in the cyber intelligence industry. Our future goals are focused on reinforcing the safeguards and processes that ensure our products are used responsibly and continuing to engage with our global stakeholders. The following are key initiatives and objectives that will guide our actions in the coming year:

1. **Deepening stakeholder engagements** – We are committed to expanding our dialogue and collaboration with a wide range of stakeholders, including civil society organizations, human rights groups, academia, and think tanks. We plan to deepen our outreach by reaching out to more civil society organizations, NGOs, and human rights defenders globally, particularly those focused on digital rights, freedom of expression, and privacy. We will aim to engage in industry-wide discussions and collaborations to promote responsible use and regulation of cyber intelligence technology, partner with law enforcement and legal organizations to explore the intersection of technology, law enforcement, and human rights, and participate in key global dialogues and conferences to influence and shape the development of industry standards that ensure the safe, ethical use of our and other similar products.

2. **Launching the product misuse investigation dashboard –** As part of our commitment to transparency and accountability, and as mentioned in the designated chapter in this report, we are developing a Product Misuse Investigation Dashboard. This dashboard will present aggregated data on the investigation process and will serve as a tool to track, monitor, and assess allegations of misuse of our products. The dashboard will centralize and streamline the investigation process, providing an efficient way to monitor ongoing investigations.

3. **Developing additional technological safeguards** – We are dedicated to further enhancing the technological safeguards embedded in our products to mitigate the risk of misuse, as mentioned in the designated chapter in this report. This includes exploring algorithmics techniques to improve the detection of misuse against vulnerable communities, and continuously refining and expanding our product compliance checks to address new and emerging risks in our field.

Alongside our new initiatives, we are dedicated to strengthening our ongoing missions, as stated in our previous reports. This includes regularly measuring the effectiveness of our human rights programs through assessments and audits, making sure they stay up-to-date with the best practices and making improvements where needed. We will continue to make sure that victims of misuse have access to clear reporting mechanisms, while also expanding transparency efforts by providing regular updates on our compliance activities and investigations. We will also work to be more transparent, sharing regular updates on our compliance activities and investigations through our public channels and product misuse investigation dashboard.

Furthermore, we remain dedicated to safeguarding human rights across all products by refining processes, conducting customer training, and strengthening contract clauses.

We are dedicated to upholding the highest ethical standards in all aspects of our operations, investing meaningful resources to ensure that our products are used responsibly and do not contribute to human rights abuses.

Our commitment to advocating for international regulation in the cyber intelligence industry remains unwavering, and we are eager to collaborate with all stakeholders to build a more responsible and ethical future for the industry.