



September 9, 2024

To The Civil Court, Thailand

Jatuphat Boonpattaraksa V NSO Group Technologies Ltd.

Case Black Number Por 3370/2566

In Response to Amicus Curiae Brief on Behalf of Amnesty International

NSO Group acknowledges the concerns raised by Amnesty International regarding the alleged misuse of our products. We recognize the gravity of these claims, and we believe it is our responsibility to address them openly, transparently, and thoroughly. Our commitment to human rights and ethical business practices is unwavering, and we wish to use this opportunity to clarify our position, reaffirm our dedication to responsible technology use, and correct any misconceptions regarding our operations.

Our commitment to human rights is not static; we continuously refine and reassess our compliance programs to stay aligned with the evolving global human rights landscape. This ongoing self-assessment process ensures that our procedures and protocols remain robust, effective, and in full compliance with the UNGP. By adhering to these principles, we strive to prevent any misuse of our technologies and to mitigate risks associated with our operations.

The Role of Cyber Intelligence and the Importance of Context

The negative discourse surrounding the cyber surveillance industry frequently overlooks the essential role our technology plays in protecting societies from significant threats such as terrorism and serious crime. Our products are crucial tools for legitimate government entities to ensure public safety and national security. These tools help combat terrorism, organized crime, and other serious threats that endanger lives and stability. The criticism directed at our industry frequently overlooks the complexity and necessity of our work, which requires a nuanced understanding of its role in safeguarding lives.

Commitment to Human Rights

At the core of NSO Group's operations is a comprehensive Human Rights Compliance Program. This program is not just a set of guidelines; it is the foundation upon which we build every aspect of our business. Our entire Human Rights Compliance Program is designed in strict accordance with the United Nations Guiding Principles on Business and Human Rights (UNGPR). These principles guide our actions and decisions, ensuring that our operations uphold the highest ethical standards and align with internationally recognized human rights norms.



Additionally, we regularly self-assess our compliance program, continuously refining it to ensure it remains robust and effective in addressing evolving human rights concerns.

Our approach begins with a thorough initial pre-sale risk assessment that evaluates the human rights conditions and governance standards of the potential customer's country. This initial assessment incorporates nine external, widely recognized governance and human rights indices, which consider factors such as human rights conditions, media freedom, rule of law, political stability, perceived levels of corruption, and government effectiveness. The evaluation of this assessment forms the basis of our comprehensive due diligence process, which includes, among other subjects, information about adverse human rights results, evaluations of domestic legal frameworks governing surveillance and data protection, and other factors such as client's foreign relations, denied parties, and other risk factors. For elevated-risk engagements, we engage with local legal experts to gain a deeper understanding of the client's domestic legal framework, and review first-hand relevant reputational information on the country and on the specific client within the country.

Following this thorough due diligence, we assign a risk classification to each customer. This classification informs a tailored mitigation plan designed to address specific risks associated with each and every customer. Depending on the risk level, these plans may include enhanced human rights training for product operators, additional contractual safeguards, and periodic audits conducted by our compliance team or independent third-party auditors. Our ongoing monitoring of public reports and additional technological restrictions, if necessary, help ensure that our products are used responsibly.

Moreover, we conduct continued oversight and monitoring of existing clients to ensure ongoing compliance with our ethical and legal standards. This includes renewing due diligence on existing customers, developing and reviewing contractual clauses, and conducting periodic compliance training. These activities are part of our commitment to maintaining high standards throughout the lifecycle of our client relationships, ensuring that our products are used responsibly and in accordance with international human rights norms.

Product Misuse Investigation Protocol

Amnesty International has claimed that NSO Group has not disclosed the details of investigations or any subsequent remedies provided to individuals affected by the alleged misuse of our products. We must be clear: Given the nature of our clients—law enforcement and intelligence agencies—and the confidentiality agreements that govern our operations, it is not possible for us to disclose or even acknowledge the existence of specific investigations. This is a fundamental aspect of our business, and it does not, in any way, diminish our commitment to investigating every credible claim of misuse.



We recognize the challenges that arise from the secrecy surrounding the cyber surveillance industry. However, the confidentiality required to protect national security and law enforcement operations does not prevent us from acting where necessary. When potential misuse of our products is reported or detected, we activate our comprehensive Product Misuse Investigation Protocol. This protocol ensures that investigations are conducted thoroughly, fairly, and transparently. We encourage both internal and external stakeholders to raise concerns through our grievance mechanisms, which include confidential and anonymous reporting channels. Our Internal Whistleblowing Policy supports employees, consultants, officers, and directors who raise concerns in good faith and protects them from retaliation. Our External Whistleblowing Policy facilitates confidential reporting by business partners, customers, and affected individuals. We also offer the option for communications through mutually agreed third parties to maintain confidentiality. This is a testament to our firm commitment to responsible technology use, even if we cannot publicly disclose the details of each investigation.

In response to the Pegasus Project claims in 2021, NSO Group clearly stated that we would continue to investigate all credible claims of misuse and take appropriate action based on the results of these investigations. This remains our position and we have acted accordingly. However, Amnesty International's assertion that we have not released the details of these investigations overlooks the critical need for confidentiality in our industry. As a company that serves government clients engaged in sensitive law enforcement and intelligence activities, we are bound by strict confidentiality agreements. This confidentiality is not a choice but a legal and operational necessity.

Proactive Outreach and Engagements

Our commitment to addressing allegations of misuse is evident in our previous responses to Amnesty International and other NGOs. We have addressed all correspondence received and investigated claims when warranted. In fact, we actively seek engagement with external stakeholders, including civil society organizations. Unfortunately, many of our outreach efforts have gone unanswered. This lack of engagement hinders our ability to address concerns collaboratively and transparently, raises concerns about a broader bias against the cyber intelligence industry, or other more grievous biases as have been publicly recorded, rather than a genuine effort to engage in constructive dialogue. This pattern of limited response undermines our ability to address concerns collaboratively and transparently.

We remain committed to fostering open communication and believe that constructive dialogue is essential to addressing the concerns of all parties involved. We continue to reach out to organizations like Amnesty International in the hope that they will engage with us meaningfully, allowing us to work together toward common goals.



Addressing Misconceptions

Despite our stringent compliance measures, we find ourselves confronted with allegations and misconceptions about our operations. One such example is Amnesty International's decision to join this case as an amicus curiae, focusing on human rights concerns associated with surveillance tools, even though there is no evidence to suggest that our products were utilized in this particular case. This raises a fundamental issue: NSO Group does not operate or utilize its products. Instead, our government clients do so under strict contractual agreements. These agreements are designed to ensure that our technology is used solely for legitimate and lawful purposes, such as combating terrorism and serious crime. The focus on NSO Group in this legal context, despite the absence of direct evidence linking our products to the alleged misuse, underscores a significant misunderstanding of our role and responsibilities. The focus on our company in this legal context, despite the lack of evidence linking our products to the alleged misuse, and ignoring our role as a software provider, highlights a broader issue of misperceptions about the company's operations.

Our efforts to engage with civil society organizations, including Amnesty International, are central to our human rights approach, but have often met with silence. We have consistently sought to engage with Amnesty International and other NGOs in constructive dialogue, share our processes, and seek input from these organizations to improve our practices. However, the lack of engagement raises concerns about whether the focus is truly on addressing human rights issues or if it stems from other agendas. This pattern of limited response undermines our ability to work collaboratively with NGOs and civil society to address concerns in a constructive manner.

Despite this, we recognize the importance of addressing concerns raised by human rights organizations and continue to welcome dialogue. While our proactive outreach to Amnesty International and other NGOs has often gone unanswered, which raises questions as to the impartiality of Amnesty as amicus curia in this case, we remain committed to fostering open communication and addressing any issues that may arise.

Setting Industry Standards

Our dedication to human rights remains unwavering. We continuously refine our processes and practices to ensure they align with international frameworks and the UN Guiding Principles. Our goal is to set a high standard within the industry, demonstrating that it is possible to uphold human rights while achieving our operational objectives. We are committed to leading by example and setting benchmarks for responsible technology use.

We are committed to setting a benchmark for responsible operations in the cyber intelligence sector and will continue to refine our practices based on real-world experience and emerging best practices. Our dedication to these principles is unwavering, and we seek to address any concerns transparently and constructively.



Conclusion

We respectfully ask the Court to consider our position in this matter and recognize the extensive efforts we have made to align our operations with internationally recognized human rights standards. Our commitment to transparency, ethical practices, and responsible technology use is unwavering, and we stand ready to address any concerns that may arise.

Sincerely,
NSO Group