January 22, 2025

To:
The Business & Human Rights Centre

We have reviewed the draft that you provided to us.

Firstly, we would like to start with some general comments regarding the report. The report does in fact highlight the obvious regarding some of the risks to investors when investing in surveillance tech. On the other hand, there are several matters that the report is lacking in order to present a more balanced picture. One cannot discuss some of the inherent risks that exist in the field without first discussing why this field exists and is necessary. In order to understand the risks, it is important for them to be discussed in light of the realities that led to the development of these technologies. One also needs to consider that these tools are used by law enforcement and other government agencies throughout the Western world and these are the main customers of the companies that develop these tools.

Over more than a decade, law enforcement and security agencies have faced a structural shift in the communications environment. The widespread adoption of end-to-end encryption, anonymization services, and reduced data retention has significantly limited the effectiveness of traditional lawful interception tools. These encryption technologies are available to all with no regulatory or compliance restrictions on who can obtain and use them.

The "going dark" challenge reflects changes in how serious criminal and terrorist activity is organized and concealed. In many cases, conventional investigative tools are ineffective even where legal thresholds for their use have been met. Cyber intelligence technologies, which you refer to by the colloquial term of "spyware", were developed as a targeted response to this gap, enabling lawful authorities, acting under applicable legal frameworks, to obtain access to information necessary to investigate and prevent the most serious threats to public safety when other means are insufficient.

This necessity is recognized in international law. Article 20 of the United Nations Convention against Transnational Organized Crime (UNTOC) expressly acknowledges the use of "special investigative techniques", including modern electronic methods, subject to domestic law, safeguards and oversight. Such tools are intended as exceptional tools, typically reserved for cases involving serious crime or terrorism, and governed by legal authorization, purpose limitation, and independent supervision.

Understanding this necessity is essential to any balanced assessment of cyber intelligence technologies. Investments should not be grounded solely in the risks associated with the potential misuses of these technology; it should also take account of the legitimate public interest in protecting lives, dismantle criminal networks, and prevent grave harm. The challenge for policymakers, regulators, industry and investors is therefore not whether investment risks exist, but how to balance this with need and how these risks may be mitigated using governance, constraint, and oversight in a manner consistent with the rule of law and respect for human rights.

NSO Group Technologies LTDI Allied Cities Tower A, Glilot, Ramat Hasharon, Israel
Telephone: +972.77.4341292 I Fax: +972.77.4253513 I I Email: office@nsogroup.com

When one understands the necessity of this tools it should actually act to encourage responsible actors to invest in companies like the NSO Group that have integrity as a core value. Though there are inherent risks in this field, they can be greatly reduced through just minded ownership, compliant behavior and adherence to international norms. Those that value a lawful and just society can view this field a great investment opportunity whilst balancing and managing the risks. Such ownership can then act as a beacon of light to the entire industry.

Furthermore, the article seems to confuse between the risk that exists with respect to the misuse of the technology by a customer and the risk to the company that develops and licenses such technologies and through them to the investor. As one example you discuss the impact caused by the abuse of the system – this is an impact that is caused to the target of the misuse of a system by the end user – this is not a direst risk to the company or the investor. To date we are not aware of any case in which damages have been awarded to a potential target from a manufacturer of this type of technology for the damages caused to it.

After these first general points we would like to point out several issues with respect to issues that related to our company:

Human rights and conflict zones – NSO operates in a highly regulated and sensitive technological domain under a tightly governed operating model and therefore does not disclose customer identities. The Company does not operate systems, select targets, or access operational data; all deployment decisions are made exclusively by sovereign authorities under their own legal frameworks and oversight.

NSO v. WhatsApp – there are several inaccuracies is your account of this lawsuit. Firstly, the facts of the case related to access to WhatsApp's servers in California and not the "hacking" of WhatsApp accounts in different countries around the world. There is a fundamental difference between the manner in which you have depicted the issue and the actual facts of the case as appear in the court records and its decisions. Secondly, the court held that there was no relevance as to the identity of the alleged targets to the outcome in the case and therefore the issue of the legitimacy or lack thereof was not discussed at trial. This was a case about WhatsApp claiming that NSO systems access their servers without authorization, not about "hacking" phones of targets. Thirdly, the court subsequently reduced the damages to less than $4,500,000. NSO is appealing the judgment.

Criminal Investigation and Lawsuits – the information is not accurate, as in several of the jurisdictions mentioned, the prosecutions opened might potentially be related to the use of systems sold by NSO Group, but NSO Group is not a target of those investigation. With respect to some of the matters NSO Group has no knowledge other than what is stated in the press, as we have not been contacted by any relevant authority.

Amazon Web Services – In statements responding to these reports. NSO Group has previously stated that many of the claims were false.

To summarize, the field of surveillance technology is indeed a complex area which requires the balancing of risks with the importance of the technology to saving lives and preventing crime. The

NSO Group is at the forefront of leading the way in how to best to mitigate the risks as demonstrated in our most recent Transparency and Responsibility Report available on our website at: https://www.nsogroup.com/wp-content/uploads/2026/01/2025-Transparency-and-Responsibility-Report.pdf

Best regards,

Chaim Gelfand, Adv.
VP Compliance and Deputy General Counsel

NSO Group Technologies LTDI Allied Cities Tower A, Glilot, Ramat Hasharon, Israel
Telephone: +972.77.4341292 I Fax: +972.77.4253513 I I Email: office@nsogroup.com