NOVALPINA

CAPITAL

Amnesty International
R3D: Red en Defensa de los Derechos Digitales
Privacy International
Access Now
Human Rights Watch
Reporters Without Borders
Robert L. Bernstein Institute for Human Rights, NYU School of Law and Global Justice Clinic, NYU School of Law

Cc: Citizen Lab

Response to Open Letter to Novalpina Capital on 18 February 2019

1 March 2019

I write in reply to your open letter to Novalpina Capital on 18 February 2019. Please consider this reply to be an open letter for you to publish and share freely. In the interests of transparency, I have also copied Citizen Lab on this correspondence as they have contacted us separately with a number of questions similar to your own, and I hope this reply will also provide them with helpful background and explanation.

I would like to state at the outset that I welcome your collective willingness to engage in informed dialogue on the governance of NSO Group ("NSO") specifically and the cybersecurity sector more generally.

In my reply, I will provide you with important context on my own background, on Novalpina Capital and on the thinking behind our decision to invest in NSO. I will then set out the steps we intend to take – together with NSO's executive management team and through engagement with human rights groups, civil society groups and other relevant stakeholders – which I believe will address over time the key points you have set out in your letter to us.

Novalpina Capital LLP, 10 Bruton Street, London W1J 6PX
+44 20 3907 4444 | info@novalpina.pe | www.novalpina.pe
A limited liability partnership registered in England and Wales
with registered number OC414979

Firstly, I want to state my own clear commitment to good corporate governance, to the rights of NGOs, journalists and dissidents to hold both governments and corporations accountable for their actions, and to the protection of human rights. Besides my relatively extensive experience in international private equity investment, I have an academic and practical background in policy relating to social justice, development, governance and anti-corruption. This included studying in 2014-2015 at the Institute of Global Affairs at Yale (on whose board I now sit) and a Visiting Fellowship at the Blavatnik School of Government at Oxford from 2016-2018. I have also been involved with a number of NGOs including Global Witness (where I was a board member from 2015 until I recently stepped down) and the Open Contracting Partnership, where I have been an Advisory Board member since 2016 and am currently Chair.

The private equity fund that I co-founded and co-lead, Novalpina Capital, is committed to operating under the highest standards of corporate governance, acting with integrity and a respect for human rights at all times. We are a signatory to the UN Principles on Responsible Investing, and we build ESG evaluations (including from a human rights perspective) into our investment decision processes and operating practices. We believe that in addition to creating financial returns for our investors, we should aim to eliminate during our ownership, as far as possible, any societal harms a business may produce.

We believe that every business in which we invest – including NSO – can and should be operated in accordance with all aspects of the UN Guiding Principles on Business and Human Rights (the "UN Guiding Principles"), including a commitment to robust transparency in line with those Principles.

We fully understand that the cybersecurity industry within which NSO operates is contentious and has concerned human rights groups for some time. I would like to set out why all of us at Novalpina Capital – with our strong commitment to human rights – believe it is right to have made this acquisition. I will also provide you with an initial outline as to how we intend to be a good, responsible and ethical owner of this company whose work (for reasons I explain below) is of such importance.

As you know, in recent years there has been a rapid growth worldwide in the use of end-to-end encrypted communications. There are very significant societal benefits associated with widespread adoption of end-to-end encryption algorithms in messaging platforms, web browsing and other forms of electronic communications. This technology enables citizens to communicate with a high degree of confidence that their fundamental human rights will be protected. As the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, concluded in his 2015 report to the UN Human Rights Council, encryption and anonymity "provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age.". End-

Novalpina Capital LLP, 10 Bruton Street, London W1J 6PX
+44 20 3907 4444 | info@novalpina.pe | www.novalpina.pe
A limited liability partnership registered in England and Wales
with registered number OC414979

to-end encryption is also vital for business, industry and government; for example, without it e-commerce and online banking could not function as no organisation would be willing to transfer funds over a potentially insecure connection.

However, the growth of end-to-end encryption – while greatly positive for the reasons I outline above – also presents society with a paradox. End-to-end encryption makes it extremely difficult for law enforcement and intelligence agencies to gain access to the content of communications between individuals intent on causing harm to the public. The bodies tasked with protecting the public from serious harms have found that their ability to identify, monitor and disrupt a wide range of criminal and terrorist activities has been degraded as a consequence of virtually unbreakable encryption. This is particularly the case for cross-border organised crime such as child sexual abuse networks, drug smuggling and human trafficking and for terrorist-related activity. In effect, the technology that protects the public is also increasingly putting the public at risk; an unintended consequence that requires a rational and proportionate discussion on the way forward.

I know that this point arouses concern among human rights and civil society groups who are worried that the inevitable direction of travel is an overall weakening of the effectiveness of end-to-end encryption and therefore an erosion of what is unarguably an important layer of protection for human rights worldwide. We fully understand that concern. We would point out, though, that if intelligence agencies and law enforcement are unable to intervene effectively when they are lawfully authorised to do so, the risk to the human rights of victims of terrorism, drug smugglers, people traffickers and child sexual abuse rings (among many other such examples) is far from inconsequential. The harms involved cannot be discounted; they are real, and growing.

In our view, a commitment to protect one aspect of human rights (the citizen's right to privacy and freedom of expression) that is strengthened by the use of end-to-end encryption must be matched by a willingness to act when it is clear that another aspect of human rights (the citizen's right to life, personal liberty, security and bodily integrity) is at risk as a result of that technology. I am sure you would agree that all fundamental human rights are equally important. In that respect, we believe that inaction to address the encryption paradox is simply untenable.

A number of law enforcement and intelligence agencies have told the company that the timely and targeted deployment of the type of technology supplied by NSO has played a direct and critical role in preventing loss of life and serious injury, including (to provide you with one recent example, the details of which cannot be disclosed for operational reasons) the disruption of plans for a terrorist attack at a crowded stadium in Europe. NSO technology is also used in a number of other public safety applications. This includes providing assistance to the Brazilian authorities in the search for the remains of people killed in the recent Brumadinho mining dam

Novalpina Capital LLP, 10 Bruton Street, London W1J 6PX
+44 20 3907 4444 | info@novalpina.pe | www.novalpina.pe
A limited liability partnership registered in England and Wales
with registered number OC414979

collapse, assisting rescue teams searching for people trapped under ruins after the 2017 Mexican earthquake, and helping the emergency services locate construction workers trapped when a parking garage collapsed in Tel Aviv in 2016.

I would also like to highlight another important aspect of our thinking in choosing to invest in NSO. For the reasons I outline above, many governments, law enforcement bodies and intelligence agencies are seriously concerned that many individuals intent on public harm are able to communicate and coordinate over end-to-end encrypted channels free from the potential of lawful agency intervention. In a number of countries, those concerns have prompted legislative debates focused on the potential for end-to-end encrypted communications to be decrypted at the core telecommunications network level so that agencies can gain access to communications content in the clear.

Network-level decryption – via so-called network 'backdoors' or man-in-the-middle decryption technologies – is fraught with enormous risk. As telecoms operators and human rights groups have pointed out, this approach would compromise overall network integrity, putting all users of those networks at risk. It would also provide governments with the capabilities required (should they choose to use them) to implement mass surveillance regimes, utilising decryption technology built into core networks to gain cleartext access to all traffic transiting across them.

We believe that any and all actions by law enforcement and intelligence agencies must be proportionate and targeted, operating within robust and clear legal frameworks. As has been reported publicly in a number of countries, the technology developed by NSO enables investigators to focus on a small number of specific individuals of concern at the device level. NSO's technology is highly targeted by design. From a human rights perspective, we believe it is a compelling alternative to what would otherwise be the seemingly inevitable outcome from current government and agency discussions worldwide: the weakening of end-to-end encryption at the network level and, in turn, the re-emergence of widespread mass surveillance regimes enabled by network 'backdoor'/man-in-the-middle decryption.

Our overall thinking in considering the human rights aspects of an investment in NSO was therefore informed by two beliefs:

1. the long-term viability of ubiquitous end-to-end encryption – with all of its benefits for the protection of human rights – depends on urgent action to address the role that end-to-end encryption also plays in facilitating human rights abuse by individuals intent on harming the public such as terrorists and criminals, and;
2. any action in this area should be proportionate and targeted, with processes in place in line with the UN Guiding Principles to mitigate any potential human rights risks arising as a consequence of that action.

Prior to making our investment in NSO, we conducted thorough due diligence on the company. In addition to a detailed assessment of the company's financial and operating data for investment purposes, our due diligence focused on its legal compliance framework and approach to a wide range of ESG matters.

The due diligence programme was led and coordinated by myself and my partner Stefan Kowski, and was supported by four investment professionals in the Novalpina Capital team. We drew on the expertise of a number of specialist external legal advisers with a background in corporate governance and international human rights, and assessed NSO's compliance with best practice in the cybersecurity industry. The external advisers involved included:

- the international law firm Weil, Gotshal & Manges (with a team of 22 lawyers under the leadership of Prof. Dr. Gerhard Schmidt) for legal compliance due diligence;
- Dr Günter Schmid (co-founder of KERBEROS Compliance Managementsysteme GmbH (https://kerberos-cms.com) and an experienced corporate executive with a background in compliance) for overall corporate governance due diligence including ESG;
- Deloitte Touche Tohmatsu Limited (with a team of approximately 20 accountants under the leadership of Mark Diffey) for financial and tax due diligence; and
- the international law firm, White & Case for financing parties' due diligence.

The design of the due diligence programme was informed by a number of human rights guidelines including the UN Guiding Principles, the European Union ICT Sector Guide on Implementing the UN Guiding Principles and UK Guidance on Assessing Cyber Security Export Risks.

We were given the opportunity to interview the NSO senior management team at length and explored with them all of the available information regarding allegations of misuse and the results of the subsequent related investigations carried out by NSO. Detailed interviews were conducted with:

- Chief Executive Officer;
- Chief Financial Officer;
- Chief Business Officer;
- Chief Product Officer;
- Chief Operating Officer;
- VP Human Resources;
- Head of Business Development; and
- General Counsel, Legal & Compliance.

We also engaged with independent members of NSO's Business Ethics Committee ("BEC"), the governance body that oversees the selection of end-user organisations and any investigations into instances of alleged misuse, as described further below.

I would add that in designing the due diligence programme ahead of our acquisition of NSO, our approach was directly informed by a detailed analysis of prior concerns and allegations expressed by human rights groups and academic research organisations in a wide range of public statements and research reports.

In your letter of 18 February, you set out your concerns regarding matters that predate Novalpina Capital's involvement with NSO. We examined NSO's approach in response to allegations of misuse of the company's technology as part of the due diligence process outlined above.

We spent four weeks engaging intensively with NSO management and the members of the BEC. We found no indication that the process followed by the company to investigate alleged misuse of its technology was partial or otherwise flawed, nor anything to substantiate the misuse allegations. We found that the company's commitment to investigating such incidents was underpinned by a significant allocation of resources, and we identified three investigations over the last three years that led to NSO deciding to terminate a contract.

I would highlight that in the cybersecurity industry, there can sometimes be an asymmetry of access to reliable information, with multiple separate parties potentially involved in a particular episode of concern. Similarly, attribution of responsibility can be a challenge when there is ambiguity about the origin and design of a particular technology. NSO is not the only company in the cybersecurity industry providing device-level capabilities to intelligence agencies and law enforcement. Nor is it necessarily the only company that makes use of a particular technique in designing such capabilities. It is therefore wholly feasible that the some of the allegations made centre on the misuse of commercial decryption technology supplied by companies other than NSO but which – in the absence of evidence to the contrary – have been deemed by human rights groups and others to be the responsibility of NSO. I would add that the number of allegations reported publicly appears inconsistent with the limited number of licences supplied by NSO to organisations authorised to deploy the company's technology, which is (as I explain above) designed to be used in a highly targeted manner.

This is not to dismiss lightly any of the claims made about past attempts to compromise devices used by human rights activists, journalists, lawyers or any other member of civil society groups. For the avoidance of doubt, we abhor any abuse of human rights of any kind, including any instance in which it were proven that human rights abuse was facilitated by the misuse of NSO's technology. As I will set out later in my reply to you, we intend to explore options to provide much greater protection

Novalpina Capital LLP, 10 Bruton Street, London W1J 6PX
+44 20 3907 4444 | info@novalpina.pe | www.novalpina.pe
A limited liability partnership registered in England and Wales
with registered number OC414979

for individuals in such roles in future.

We understand fully our responsibilities under s.15(c) ("processes to enable the remediation of any adverse human rights impacts") and s.22 ("where business enterprises identify that they have caused or contributed to adverse impacts, they should provide for or cooperate in their remediation through legitimate processes") of the UN Guiding Principles. As part of our work to strengthen the current governance framework at NSO to bring this into line with the UN Guiding Principles, we will address the requirement for remediation (including for any substantiated historic abuses) as stipulated under the Principles.

You also ask for more information about the current management structure, governance processes and operating procedures of NSO. At this point prior to the closing of the acquisition, we are prohibited under the terms of our sale and purchase agreement and non-disclosure agreement with NSO from disclosing certain information relating to the company and the acquisition. Once the acquisition has closed – and as part of our commitment to robust transparency in line with the Guiding Principles – we will move to a much greater level of disclosure than is possible at this point.

I will summarise below the key points as far as I can at this stage. Before I do so, I would emphasise again that this is simply a snapshot of the status quo. As I explain later in my reply, we intend to build on these arrangements significantly in future.

Ownership and Board composition

Post the closing of the acquisition, a fund managed by Novalpina Capital will hold the majority of the shares in NSO, with management and the company's founders owning the balance. The Board of Directors will comprise representatives from Novalpina Capital (including myself) and the NSO management and founders. The Board of Directors will be ultimately responsible for the governance of the company. I will chair the Board. The executive management team will be appointed by the Board of Directors and report to it. Once the acquisition has closed, we will make public the names and backgrounds of the Directors on the Board as well as the executive leadership team.

Export controls

The very large majority of contracts with end-user organisations to deploy NSO's technology under licence require an export licence from the government of country of export. Export licences are typically (although not exclusively) granted by the Israeli authorities. Although Israel is not a signatory to the Wassenaar Arrangement, the Israeli authorities apply the Wassenaar control lists in administering export controls and closely regulate the companies involved. NSO's end-user technology is

Novalpina Capital LLP, 10 Bruton Street, London W1J 6PX
+44 20 3907 4444 | info@novalpina.pe | www.novalpina.pe
A limited liability partnership registered in England and Wales
with registered number OC414979

regulated by the Israeli Defense Export Control Agency ("DECA"), and NSO is registered with DECA.

The first step in engaging with potential end-user organisations in a new market involves securing a marketing licence from DECA which permits sales staff to visit the country to enter into discussions, up to and including negotiating a purchase agreement. At that stage, an export licence is then required to proceed any further with the transaction. The application to DECA for an export licence is accompanied by an End-User Undertaking ("EEU") signed by the ultimate end-user of the technology. The EEU includes information relating to the use of the system, the identity of the end-user, and undertakings that the system will not be transferred to any other user. DECA carries out periodic audits of NSO's facilities to ensure compliance with its rules and record keeping requirements. Our due diligence confirmed there have been no adverse findings from those audits.

Some of NSO's products are exported from the EU (either Bulgaria or Cyprus), where the relevant authorities apply the EU control list (which is based on the Wassenaar control list). For every sale, a consultation is held with the appropriate authority to determine whether or not an export licence is necessary, with such a licence then obtained if required.

Business Ethics Committee

Any form of marketing engagement or proposed contract that is assessed to be compliant with export control rules under the regulatory regime summarised above must then be reviewed by the NSO Business Ethics Committee (the "BEC") before proceeding.

The BEC is a key Committee of the NSO Board and comprises seven members: three NSO executives, and four external independent members. The external independent members are individuals of international standing in the fields of law, technology, security and international relations that are relevant to NSO's business activities.

The BEC has the final say over whether or not NSO will enter into a contract with an end-user organisation; without the Committee's approval, purchase agreements with potential end-user organisations will not proceed to signed contracts.

The BEC's mandate is focused purely on matters of ethics; factors such as commercial value are extraneous to its discussions and decisions. The Committee considers all ethical matters including the potential for the risk of misuse of the company's technology and consideration of any related human rights aspects. Those considerations include assessing the extent of risk that a particular government or agency could misuse NSO technology to target journalists, political opponents or other critics. The Committee takes account of a broad range of inputs and

Novalpina Capital LLP, 10 Bruton Street, London W1J 6PX
+44 20 3907 4444 | info@novalpina.pe | www.novalpina.pe
A limited liability partnership registered in England and Wales
with registered number OC414979

considerations in its decision-making process, including undertaking research that may take several months to complete.

The BEC regularly declines the opportunity for new contracts on ethical grounds. As has been publicly stated by NSO in previous media reports, the company has rejected more than $100 million of potential contracts over the last three years, with significantly more deferred for further review. This is in the context of company revenues in 2018 of $250 million. The BEC also must approve the renewal of maintenance contracts.

End-user organisation contracts

NSO enters into detailed contracts with the end-user organisations licensed to deploy NSO technology. Under the company's standard-form contract, the end-user organisation is subject to comprehensive compliance obligations stipulating that use of NSO technology must comply with all applicable laws including those related to privacy and national security. Furthermore, the contractual terms state clearly that NSO technology is to be deployed in order to prevent and investigate crime and terrorism and must not be used in a manner which violates human rights.

Investigation of claims or suspicion of misuse

As I stated earlier in summarising the due diligence undertaken by Novalpina Capital, NSO has a process in place to investigate whenever it becomes aware of a potential misuse of its technology. A team consisting of between 5 and 10 people (depending on the complexity of the matter under investigation) is convened and takes immediate action to seek to secure the necessary evidence. That team involves members drawn from the R&D department and operational team with guidance and support from members of NSO senior management and the in-house legal team. The most complex investigations are overseen by the general counsel of NSO, who provides briefings to the BEC and the NSO Board on progress.

The process typically consists of three parallel workstreams: operational, technical and legal/compliance. Investigations typically reach a conclusion within 2-4 weeks, and every step is documented.

- *Operational Workstream*: the investigation team may meet the end-user organisation suspected of misuse in order to conduct interviews and gather detailed information. Investigation meetings typically include the head of the organisation in question together with senior members of NSO management and an NSO legal representative. These meetings go into the detail of alleged misuses, including in many cases asking the organisation's representatives to explain the legal process they followed in specific use cases, together with an explanation of the permissions required from relevant authorities for any

Novalpina Capital LLP, 10 Bruton Street, London W1J 6PX
+44 20 3907 4444 | info@novalpina.pe | www.novalpina.pe
A limited liability partnership registered in England and Wales
with registered number OC414979

such actions. The investigation team will also typically meet senior government officials to cross-reference information supplied by the organisation involved, and to ask additional questions.

- *Technical Workstream*: with the permission of the end-user organisation under investigation, NSO R&D department investigators access the audit database of the organisation's system to review operational data relevant to the alleged misuse case. The searches are conducted at arm's length (by design, NSO investigators do not have access to any private communications data) against parameters provided by the complainant, whistle-blower or other sources.

- *Legal/compliance workstream*: The legal and compliance team monitors the progress of NSO's investigations and receives input from the BEC and the company's Board of Directors on a regular basis. If the investigation identifies evidence of misuse of NSO's technology (and therefore a breach of the licence conditions), NSO can suspend or curtail an end-user organisation's technology licence while the investigation continues. At the end of an investigation, NSO management and the BEC review the findings. If the conclusion is that there is proven misuse of NSO's technology, the organisation's licence is immediately suspended.

You also asked for a number of assurances about our plans for NSO Group in future.

NSO already operates under an ethical governance framework that is significantly more robust than any of its peers. This is one of the reasons why we first contemplated acquiring the business. Our intention is to build on that framework to bring the company's governance and operating procedures into line with the UN Guiding Principles. We are also following closely the submissions from civil society groups to the United Nations Special Rapporteur David Kaye in preparation for his report to the General Assembly in October 2019 and will take the recommendations in those submissions into account in developing our approach, as well as those that will be issued later this year by the Special Rapporteur. The strengthened governance framework for NSO will include a robust transparency programme that will be in line with s.21 of the Principles.

Once the transaction has closed, we will be supported in this work by a number of specialist external advisers with a background in corporate governance, ESG, human rights and transparency.

We will also commission an independent Human Rights Impact Assessment (HRIA) to ensure that the governance framework reflects a comprehensive external analysis of all associated human rights risks and is fully informed by the concerns of all stakeholders, including human rights NGOs and other civil society groups. We will

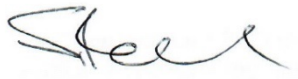
Novalpina Capital LLP, 10 Bruton Street, London W1J 6PX
+44 20 3907 4444 | info@novalpina.pe | www.novalpina.pe
A limited liability partnership registered in England and Wales
with registered number OC414979

publish the findings of the HRIA as part of our broader commitment to robust transparency.

The governance framework will include additional safeguards to ensure that technology designed to save life and protect the public from harm is not also misused to undermine other fundamental human rights including privacy and freedom of expression. I would add that we are particularly mindful of the work of human rights activists, journalists, lawyers and members of other civil society groups. Current NSO technology licence conditions already expressly prohibit the misuse of the company's technology, and we intend to explore further measures to protect those who find themselves vulnerable to human rights abuse for no reason other than their commitment to protect human rights.

I hope all of the above provides you with some assurance that we approach our investment in NSO with a strong commitment to the protection of human rights. Your experiences, insights and guidance will be invaluable in helping to shape our understanding of the future for NSO as a highly ethical and responsible company grounded in a respect for human rights – setting the standard for its industry. We would greatly welcome direct engagement with all of you to discuss this further.

Yours sincerely,



Stephen Peel
Founding Partner
Novalpina Capital

Cc:
Stefan Kowski – Founding Partner, Novalpina Capital
Bastian Lueken – Founding Partner, Novalpina Capital
Shalev Hulio -CEO and Founder, NSO
Francisco Partners