

OPERATING FROM THE SHADOWS

INSIDE NSO GROUP'S CORPORATE STRUCTURE

A briefing by Amnesty International, Privacy International and The Centre for Research on Multinational Corporations (SOMO)

SOMO

PRIVACY INTERNATIONAL

AMNESTY INTERNATIONAL

Amnesty International is a movement of 10 million people which mobilizes the humanity in everyone and campaigns for change so we can all enjoy our human rights. Our vision is of a world where those in power keep their promises, respect international law and are held to account. We are independent of any government, political ideology, economic interest or religion and are funded mainly by our membership and individual donations. We believe that acting in solidarity and compassion with people everywhere can change our societies for the better.

Privacy International was founded in 1990 and is based in London, UK. It was the first organization to campaign at an international level on privacy issues. It is committed to protecting people's privacy, dignity and freedoms from abuses by companies and governments. Through research, litigation and advocacy, it works to build a better future where technologies, laws, and policies contain modern safeguards to protect people and their data from exploitation.

SOMO investigates multinationals. Independent, factual, critical and with a clear goal: a fair and sustainable world, in which public interests outweigh corporate interests. We conduct action-oriented research to expose the impact and unprecedented power of multinationals. Cooperating with hundreds of organisations around the world, we ensure that our information arrives where it has the most impact: from communities and courtrooms to civil society organisations, media and politicians.

© Amnesty International, Privacy International, and The Centre for Research on Multinational Corporations (SOMO) 2021
Except where otherwise noted, content in this document is licensed under a Creative Commons (attribution, non-commercial, no derivatives, international 4.0) licence.
https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode
For more information please visit the permissions page on our website: www.amnesty.org
Where material is attributed to a copyright owner other than Amnesty International this material is not subject to the Creative Commons licence.

First published in 2021 by Amnesty International Ltd
Peter Benenson House, 1 Easton Street, London WC1X 0DW, UK

Index: DOC 10/4182/2021
Original language: English
amnesty.org

Cover illustration: © Toscanabanana 2021

CONTENTS

1. EXECUTIVE SUMMARY 4

2. GLOSSARY 9

3. METHODOLOGY 11

4. OVERVIEW: THE GLOBAL SURVEILLANCE INDUSTRY, INTERNATIONAL HUMAN RIGHTS LAW, AND EXPORT REGULATIONS 12

4.1 WHAT IS THE GLOBAL SURVEILLANCE INDUSTRY? 12

4.2 HUMAN RIGHTS LAW APPLICABLE TO STATES AND COMPANIES 15

4.3 EXPORT REGULATIONS APPLICABLE TO THE DIGITAL SURVEILLANCE INDUSTRY 17

5. MOUNTING EVIDENCE OF SURVEILLANCE ABUSES INVOLVING NSO GROUP TECHNOLOGY 25

6. THE NSO CORPORATE STRUCTURE 29

6.1 WHAT IS "NSO GROUP"? 29

6.2 THE FRANCISCO PARTNERS YEARS (2014-2019) 31

6.3 OWNERSHIP CHANGES IN 2019 42

7. APPLYING THE RESPONSIBILITY TO RESPECT HUMAN RIGHTS ACROSS THE NSO CORPORATE FRAMEWORK 59

8. CONCLUSION 62

9. RECOMMENDATIONS 64

10. ANNEXES 66

1. EXECUTIVE SUMMARY

Targeted surveillance is a serious threat facing human rights defenders (HRDs) globally. Though often carried out by states, this practice is enabled by digital surveillance tools provided by private companies. However, the lack of transparency about the operations of the surveillance industry poses a serious obstacle for victims of unlawful surveillance to seek accountability and the right to remedy. This briefing seeks to shed light on one specific company – NSO Group – and thereby help to overcome this barrier.

Targeted surveillance is the practice of putting under surveillance specific persons who may be of interest to authorities, either remotely using digital surveillance technologies, or by following and watching them in person, or a combination of the two. Among many other tactics, targeted digital surveillance can involve government hacking – when authorities compromise a targeted person's devices by exploiting system or software vulnerabilities to install malware and spyware – or compromising digital communications through phishing campaigns. State intelligence and law enforcement agencies may legitimately engage in surveillance in order to acquire information essential to protect and prevent threats to the public, so long as such surveillance activities are undertaken in compliance with international human rights law and standards.[1] Yet, while governments have used targeted digital surveillance to fight crime and terror, some have also used it to target HRDs, compromising their digital devices in order to monitor their activities and communications, obtain access to their private data, and ultimately undermine and/or persecute those targeted.[2] Rhetoric around the necessity of surveillance technologies has frequently failed to grapple with these documented, illegitimate parallel uses.

Although it is possible that some governments manufacture tools to conduct targeted digital surveillance themselves, many states buy the sophisticated technology enabling such surveillance from private companies. They justify the procurement of these technologies as essential for maintaining law and order. Some of these surveillance companies manufacture and sell spyware or other such tools to states, who have, in addition to legitimate purposes, used surveillance to shrink the space for dissent by targeting HRDs, in violation of their internationally recognized human rights. Targeted digital surveillance attacks of this kind involve the interplay of several state and non-state actors, including private companies, investors, law enforcement and intelligence agencies, national export control authorities, and multilateral export control regimes such as those embodied in the Wassenaar Arrangement and the EU Dual Use Regulation. Despite the human rights obligations or responsibilities

1. UN General Assembly, Resolution on nuclear disarmament, UN Doc. A/69/37, paras 6-7 & 11 ("The fact that something is technically feasible, and that it may sometimes yield useful intelligence, does not by itself mean that it is either reasonable or lawful (in terms of international or domestic law)."), https://undocs.org/A/69/37; UN Human Rights Council, *The right to privacy in the digital age*, UN Doc. A/HRC/27/37, paras 15 & 21-30, https://undocs.org/A/HRC/27/37

2. Amnesty International, *When is targeted surveillance wrong?*, 6 October 2020, www.amnesty.org/en/latest/campaigns/2020/10/stopspying/

of each of these actors, gaps in regulation, abuses by state agents, and state and corporate secrecy make it nearly impossible to identify, prevent or seek redress for the human rights abuses caused by these attacks, including by establishing adequate oversight mechanisms.

Even after years of evidence-gathering demonstrating the negative human rights impact of digital surveillance technologies – from the reported use of French company Amesys' surveillance equipment in Libya during the Arab Spring,[3] to the current revelations of targeting of journalists globally[4] – the UN Special Rapporteur on freedom of opinion and expression recently concluded that the surveillance industry continues to provide its services "unsupervised and with something close to impunity."[5]

Little is known about the surveillance industry, as it operates from the shadows despite repeated calls for more transparency and accountability.[6] This lack of transparency is a foundational challenge to human rights accountability. Without more information about the surveillance industry – for example the jurisdictions in which it operates; the identities and ownership of the companies facilitating government surveillance; the capabilities on offer; the scale of deployment; or details of company due diligence or remediation efforts – it is impossible to ascertain the full scope of the human rights risks presented, mitigate those risks, or seek remedy when abuses occur. As the UN Special Rapporteur on freedom of opinion and expression noted in his 2019 report, "Credible allegations have shown that companies are selling their tools to Governments that use them to target journalists, activists, opposition figures and others who play critical roles in democratic society. The gravity of the allegations demands transparency in companies' relationships and processes."[7]

For example, as surveillance technologies are capable of interfering with privacy, accessibility of information regarding the technical capabilities of these tools can be a safeguard against abuse.[8] An understanding of how corporate decisions are taken, and by whom, is essential to accountability of companies. As noted by the UN Special Rapporteur on freedom of opinion and expression, when companies make claims in the absence of transparency regarding the ability of their internal mechanisms to prevent these types of abuses, there is "no particular reason to take private companies at their word without subjecting them to public disclosure and accountability processes."[9]

The challenges of transparency and accountability in the surveillance industry are illustrated by the case of one of its well-known participants, NSO Group. As detailed in this briefing, research has linked the products and services of NSO Group to violations of internationally recognized human rights across the globe. NSO Group, however, has yet to be held accountable in connection with such violations (though lawsuits are pending). The company has resisted sharing even basic information about its operations, sales and service agreements, or investigations into alleged misuse, even while touting its purported "industry-leading" commitment to the UN Guiding Principles on Business and Human Rights. Simultaneously, investment in NSO Group by private equity firms – themselves largely opaque and subject to little oversight – has compounded and entrenched this lack of transparency while facilitating the growth of the NSO Group enterprise.

---

3. P. Sonne & M. Coker, "Firms Aided Libyan Spies," *Wall Street Journal*, 30 August 2011, www.wsj.com/articles/SB10001424053111904199404576538721260166388

4. B. Marczak et al., "Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit", *The Citizen Lab,* 20 December 2020, https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/

5. Report of the Special Rapporteur on freedom of opinion and expression, UN Doc. A/HCR/41/35, www.undocs.org/A/HRC/41/35

6. Amnesty International, *Open letter to Novalpina Capital, CC: NSO Group, Francisco Partners* (18 February 2019), www.amnesty.org/en/latest/research/2019/02/open-letter-to-novalpina-capital-nso-group-and-francisco-partners

7. Report of the Special Rapporteur on freedom of opinion and expression, UN Doc. A/HCR/41/35, www.undocs.org/A/HRC/41/35, p.14.

8. *Roman Zakharov v. Russia* (47143/06), European Court of Human Rights Grand Chamber (2015), para. 241; see also, Report of the Special Rapporteur on freedom of opinion and expression, Un Doc. A/HRC/23/40, para. 91, ("States should be completely transparent about the use and scope of communications surveillance techniques and powers."), www.undocs.org/A/HRC/23/40

9. Report of the Special Rapporteur on freedom of opinion and expression, UN Doc. A/HCR/41/35, www.undocs.org/A/HRC/41/35

This briefing is jointly written by Amnesty International, Privacy International and The Centre for Research on Multinational Corporations (SOMO) to detail the complex corporate structure of NSO Group – how it has changed over time and continues to change, reflecting the evolution and effects of private sector participation in state surveillance. The lack of transparency around NSO Group's corporate structure and the lack of information about the relevant jurisdictions within which it operates are significant barriers in seeking prevention of, and accountability for, human rights violations linked to NSO Group's products and services. For example, without identifying the participants in the industry, across corporate hierarchies and jurisdictions, it is not possible to understand which laws apply to their activities. In addition, without knowing the purpose or role of each company and what products and services each of those entities offer it is near impossible to assess relevant applicable export controls, or whether domestic surveillance laws are capable of adequately safeguarding against the abuse of the specific surveillance tools employed. Finally, accountability requires understanding which individuals and entities control the activities of the company or otherwise make critical decisions impacting human rights outcomes (for example, board members, owners, etc.). It also requires companies to "know and show" *how* they respect human rights,[10] in order to assess whether their commitments align with real practice.

The overall objective of this briefing is to aid civil society efforts toward greater oversight, remedy and accountability by collecting information on NSO Group's corporate structure, including information concerning ownership, control, and exports of the company, in one accessible resource in furtherance of transparency. Amnesty International, Privacy International and SOMO do not aim to draw conclusions or make assertions about the purpose of the corporate structure. A detailed analysis of the human rights implications of the corporate structure, financial flows and any tax implications are beyond the scope of this briefing and warrant further research.

The details of NSO Group's corporate structure have been obtained from subscription databases providing financial and corporate information, company registries in various jurisdictions, and by building on previous research undertaken by civil society organizations and journalists. They are non-exhaustive and do not exclude that other corporate entities and interconnections could be uncovered with further research, particularly as NSO Group's structure continues to evolve.

The briefing begins with an overview of the global surveillance industry, and applicable international human rights law and export regulations. We highlight the need for greater transparency with respect to, and human rights-based criteria for evaluation of, surveillance exports,[11] with recent proposed changes to the EU export regulations representing some progress in that direction.[12] The briefing then provides background information on NSO Group, and highlights evidence collected thus far by researchers, journalists, activists and others regarding the misuse of its tools as well as legal actions based on such evidence. The briefing then illuminates details of the corporate structure behind NSO Group, describing the multijurisdictional network of companies, investors and individuals that together make up the operational, financial and decision-making apparatuses of this surveillance technology enterprise. The last part of the briefing assesses how the corporate responsibility to respect human rights bears on the various aspects of NSO Group's business.

This briefing details the many changes over time to the NSO Group corporate structure, from its incorporation in Israel in 2010, through the purchase of a majority stake in the company by US private

10. See Principle 15, Guiding Principles on Business and Human Rights, www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

11. See CAUSE (Coalition Against Unlawful Surveillance Exports), *Shared Statement on the Update of the EU Dual-Use Regulation*, 2017, www.accessnow.org/cms/assets/uploads/2017/05/NGO_Sharedstatement_dualuse_May2017.pdf

12. B. Immenkamp, *Briefing: EU Legislation in Progress: Review of Dual-Use Export Controls*, European Parliamentary Research Service, 2021, www.europarl.europa.eu/RegData/etudes/BRIE/2016/589832/EPRS_BRI(2016)589832_EN.pdf

equity firm Francisco Partners in 2014, to the management buyout backed by UK private equity firm Novalpina Capital in 2019. It flags the various jurisdictions within which NSO Group and its various operating entities and holding companies are located, including the following countries: **the British Virgin Islands, Bulgaria, the Cayman Islands, Cyprus, Israel, Luxembourg, the UK, and the US.** We know from previous research and litigation efforts that one or more of NSO Group's entities are granted export licences in Israel as well as Bulgaria;[13] NSO Group has confirmed that its corporate entities export from Israel, Bulgaria, and Cyprus.[14] The briefing also highlights some of the investors that have a stake in NSO Group. These include two public funds based in the **UK: South Yorkshire Pensions Authority and East Riding Pension Fund;** and two based in the **US: Oregon Public Employees Retirement System and Alaska Permanent Fund Corp.** In addition, there are a number of private individuals and investor groups who have invested in NSO Group.

We assess that greater transparency in the surveillance industry – in particular, around corporate structure and offerings; exports and sales; and company decision-making apparatuses, human rights policies and processes – would advance the interests of a number of stakeholders. Transparency is a key part of corporate responsibility for human rights due diligence, and can bolster the goal of accountability and oversight of surveillance technology.[15] Potential investors in private surveillance companies would likewise benefit from accessing information crucial to understanding investment risks and impacts, and fulfilling their own responsibilities and commitments to respect human rights. Investors would be able to make more informed choices if they had access to information that ensured their investments were not violating human rights. In addition, information about the corporate structure and sales of surveillance companies facilitates oversight of state export licensing practices and access to remedy. Civil society, journalists, lawyers, surveillance victims and others can use such basic facts to determine which jurisdiction is relevant in a given case – that is, which country's export controls and other laws and regulations apply.

We recommend that **states** (a) implement the UN Special Rapporteur's call for an immediate moratorium on the global sale and transfer of the products of the private surveillance industry until rigorous human rights safeguards are put in place to regulate such practices;[16] (b) adopt and enforce a legal framework requiring private surveillance companies to conduct human rights due diligence in their global operations, supply chains and in relation to the use of their products and services; (c) adopt and enforce a legal framework requiring transparency in the key areas noted above by private surveillance companies; (d) disclose contracts with such companies and implement human rights-based procurement standards; (e) effectively regulate the export of surveillance technologies in a manner that prevents human rights abuses; (f) adopt and enforce domestic legal frameworks that create human rights safeguards against surveillance abuses and accountability mechanisms for victims of such abuses; and (g) participate in key multilateral efforts (e.g. in support of the UN Special Rapporteur's call for an immediate moratorium on the sale, transfer and use of surveillance technology) to integrate human rights standards in the development, sale and transfer, and use of surveillance technology.

---

13. See Columbia Global Freedom of Expression, Case Law: *Malekar v. DECA*, Columbia University, 12 July 2020, https://globalfreedomofexpression.columbia.edu/cases/malekar-v-deca/; Republic of Bulgaria Ministry of Economy, "Публичен регистър на лицата, регистрирани за износ и трансфер на изделия и технологии с двойна употреба [Public register of persons registered for export and transfer of dual-use items and technologies]," www.mi.government.bg/files/useruploads/files/exportcontrol/registar_iznos_transfer_22112018.xls, at rows 37 and 61; Novalpina Capital, Response to Open Letter to Novalpina Capital on 18 February 2019, 1 March 2019, www.amnesty.org/download/Documents/DOC10021022019ENGLISH.PDF

14. NSO Group Technologies Ltd. Response to Amnesty International, Privacy International, and The Centre for Research on Multinational Corporations (SOMO) letter, 2 May 2021, at Annex 4.

15. Report of the Special Rapporteur on freedom of opinion and expression, UN Doc. A/HCR/41/35, para. 60, https://undocs.org/A/HRC/41/35

16. Report of the Special Rapporteur on freedom of opinion and expression, UN Doc. A/HCR/41/35, paras. 48-49, https://undocs.org/A/HRC/41/35

We further recommend that **surveillance companies** implement a broad range of human rights due diligence, transparency, and accountability measures, in accordance with the UN Guiding Principles on Business and Human Rights and the OECD Guidelines for Multinational Enterprises. We finally recommend that **investors** assess whether their investment portfolios include or may in the future include surveillance companies, and demand that any such portfolio companies fulfil their responsibilities to respect human rights in accordance with the UN Guiding Principles and OECD Guidelines.

2. GLOSSARY

DUAL-USE ITEM	Originally defined as a product which can be used for both civilian and military purposes without modifications, it now also refers to a product with a high level of technological capabilities and security risks which is listed in international non-proliferation agreements. If a product is deemed to be a dual-use item, it is typically included within the scope of export control frameworks.
EXPLOITS	Exploits are a type of software designed to take advantage of a security flaw or weakness on computer devices ('vulnerabilities' – see below). Exploits are typically used for malicious purposes, such as compromising mobile devices by installing spyware.
HOLDING COMPANY	A corporate entity that owns or holds a stake in, and exercises control over, other companies.
MALWARE	Malicious software that is designed to be secretly installed on a victim's computer or phone with the intent to gain access to private information, damage devices and/or disrupt traffic.
NETWORK INJECTION	A type of digital attack that allows an attacker to monitor and hijack traffic such as web requests. Unlike phishing messages, this kind of attack does not require the victim to click on anything. This allows them to change the behaviour of a targeted device, including re-routing a normal request to malicious exploit pages without requiring any extra interaction from the victim.
OPERATING COMPANY	A corporate entity of which the primary function is not to hold or own another company but to manufacture a product or provide a service that it sells to its customers or clients.
PHISHING	A malicious effort to masquerade as legitimate services (such as Gmail or Facebook) in order to collect the usernames and passwords of the victims, who are usually targeted by being sent links to fake login pages.
SHARE CLASS	A designation (such as "Class A," "Class B," etc.) applied to different company shares which are distinguishable on the basis of particular rights or privileges associated with those shares (for example, voting rights, dividends, etc.).
SOPHISTICATED INVESTORS	Investors with high net worth and significant experience in financial markets that are capable of evaluating investment risk, for example, investment funds.
SPYWARE	A particular kind of malware that is designed to surreptitiously monitor the victim's computer or phone, providing an attacker access to communications, private information and files.

SS7	Signaling System No. 7 (SS7) is a set of protocols used at the core of the public switched telephone network.
VULNERABILITIES	A vulnerability is a weakness or a security flaw in a computer system or software, which can be exploited or taken advantage of to gain control of devices.
ZERO-DAY VULNERABILITIES	Zero-day vulnerabilities are security flaws that are unknown to the vendor or developer of the compromised technology.

3. METHODOLOGY

Information about NSO Group's corporate structure has been obtained from the following sources:

- Subscription databases that provide corporate information, including Moody's Orbis and Thomson Reuters' Eikon;
- Official company filings and other material obtained online and from company registers in Bulgaria; the Cayman Islands; Cyprus; Israel; Luxembourg; the Netherlands; the UK; and the US.
- Company filings to the US Securities and Exchange Commission (SEC);
- Open source datasets including Open Corporates, Organized Crime and Corruption Reporting Project (OCCRP), Open Gazettes, and Wikileaks;
- Public information available on company websites and in news reports.

These documents span the years 2010-2021, from incorporation filings to decisions taken at annual or extraordinary general meetings, to statutes or articles of association filings, including announcements of changes in key interests or people. Where possible, web links to these sources have been included in the footnotes. When this is not possible, such as when we reference documents from registers and subscription databases, the name of the document is included in the footnote. Corporate documents filed in Luxembourg, which documents are available through the Luxembourg Registre de Commerce et des Sociétés and/or the European e-Justice Portal, are collected and organized in a public folder.

After detailing the corporate structure, Amnesty International, Privacy International and The Centre for Research on Multinational Corporations (SOMO) invited the entities and individuals named in this briefing to officially respond, as well as to answer questions that were raised during the course of this research. Responses received have been incorporated within the text where relevant. Additionally, responses received from Francisco Partners and NSO Group Technologies Ltd. are included in their entirety in the Annexes.

The corporate structure documented in this briefing is non-exhaustive and may contain gaps. The companies involved are private, which means various pieces of documentation, including for example shareholder agreements or loan agreements, are not publicly available since these contract agreements are negotiated by the companies, their lawyers, bankers or financial advisors, and are held privately. Official company filings deposited in business registers have been key in uncovering the overall corporate structure and shareholder relations for the NSO group of companies. In some cases, it has not been possible to obtain company records or filings in light of company laws in certain jurisdictions, for example the Cayman Islands and the British Virgin Islands. Eikon and Orbis datasets have been helpful in piecing corporate puzzles together, but these databases are not as current as the most recent company filings, mostly in Luxembourg.

Finally, further analysis of the human rights implications of the structure, financial flows, share allocation and tax consequences of the corporate structure are outside of the scope of this briefing, but merit future investigation, research and discussion.

4. OVERVIEW: THE GLOBAL SURVEILLANCE INDUSTRY, INTERNATIONAL HUMAN RIGHTS LAW, AND EXPORT REGULATIONS

4.1 WHAT IS THE GLOBAL SURVEILLANCE INDUSTRY?

Across the world right now, governments are cracking down on dissent and preventing HRDs, activists, journalists and lawyers from carrying out their work. They are threatened and attacked using a range of tactics and tools. One tactic that occupies a prominent space in government strategies across the world is that of targeted digital surveillance, which includes government hacking.[17]

The type of government hacking enabled by NSO Group's spyware (and the spyware produced by other similar companies) is a powerful and flexible technique that presents unique and serious threats to both privacy and security.[18] It enables the collection and analysis of highly personal data that individuals might have never wished to communicate over a computer network to another, such as private notes, diaries, photographs and other biometric data, credit card data, research material, or information covered by journalistic or legal professional privilege.[19] Hacking permits governments to edit, delete, modify or falsify data on a device. It can also be used to recover data that has been deleted, send fake communications or data from the device, or add or edit code to add new capabilities or alter existing ones and erase any trace of the intrusion. In a world where information about us is increasingly expressed as data, minute changes to that data – a password, GPS co-ordinates, a document – can have radical effects. Government hacking is therefore not simply a passive technique of interception; it can be used to substantively interfere with individuals' lives.

17. See Amnesty International, *Ending the targeted digital surveillance of those who defend our rights: A summary of the impact of the digital surveillance industry on human rights defenders* (Index: ACT 30/1385/2019), www.amnesty.org/en/documents/act30/1385/2019/en/

18. Privacy International, *Government Hacking*, (n.d.), https://privacyinternational.org/learning-topics/government-hacking

19. *Privacy International and Others v. United Kingdom*, Appl No. 46259/16, Decision, ECtHR 7 July 2020, https://hudoc.echr.coe.int/eng?i=001-204588

Computer systems, especially computer software programmes, are complex. Inevitably, they contain vulnerabilities. People are also complex and their interactions with systems also give rise to vulnerabilities. Hacking operations rely to a great extent on the exploitation of system vulnerabilities, such as zero-day vulnerabilities. In the surveillance context, the companies identify vulnerabilities, not to secure systems through testing and co-ordinated disclosure, but to exploit them to facilitate a surveillance objective. This activity may not only undermine the security of the target system but also of other systems presenting serious threats to the security of multiple users of that system.

Importantly, even as private companies and their investors build a multibillion dollar industry for the provision of advanced surveillance technology, and propagate dangerous intrusion techniques, the legal foundations of the industry have never been settled. The legality of states' use of this surveillance technology is far from clear. As explained by the UN Special Rapporteur on freedom of opinion and expression:

> **"It is insufficient to say that a comprehensive system for control and use of targeted surveillance technologies is broken. It hardly exists. While human rights law provides definite restrictions on the use of surveillance tools, States conduct unlawful surveillance without fear of legal consequence. The human rights law framework is in place, but a framework to enforce limitations is not. It is imperative, urgently so that States limit the uses of such technologies to lawful ones only, subjected to the strictest forms of oversight and authorization, and that States condition private sector participation in the surveillance tools market – from research and development to marketing, sale, transfer and maintenance – on human rights due diligence and a track record of compliance with human rights norms."[20]**

Moreover, a legal basis for permitting a private company to develop and traffic in digital surveillance technology has never been spelled out. In private contexts (not involving use by state actors) such activity is generally prohibited: international and domestic law generally provide that access to or interception of digital devices is only permissible when authorization of or legal right to such access or interception is in place, for example when undertaken with consent of the device owner or as part of a properly authorized criminal investigation.[21] Indeed, digital surveillance companies have frequently asserted that they restrict sales and services to government clients only – implying the propriety and legality of their business on the basis that, if their client is a state organ, its purchase and use of surveillance technology is inherently permissible. As evidence gathered over the years has demonstrated, however, such presumption is wholly unwarranted, with state entities regularly undertaking domestic surveillance in violation of international human rights law and even, in many cases, of domestic legal frameworks. In addition, states have engaged in *extraterritorial* surveillance that appears to be conducted indiscriminately and potentially in violation of the laws and criminal procedure requirements of the state in which the victim is located.

---

20. Report of the Special Rapporteur on freedom of opinion and expression, UN Doc. A/HCR/41/35, para. 46, https://undocs.org/A/HRC/41/35

21. Under the Budapest Convention on Cybercrime (ratified by 63 states including Israel, the US, Canada and most of Europe), state parties are required to adopt measures to criminalize intentional "access to the whole or any part of a computer system without right" (Art. 2) and "interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system" (Art. 3). Moreover, state parties are to criminalize, "when committed intentionally and without right:

a) the production, sale, procurement for use, import, distribution or otherwise making available of:
   i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;
   ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5" (Art. 6(1)).

Such laws are fairly commonplace in state domestic environments, for example, the Computer Fraud and Abuse Act and the Wiretap Act in the US. (Note, however, that Israel has entered a reservation "not to apply Article 6, paragraph 1, when the offence concerns procurement for use or import.")

Additionally, the techniques and operating methods of the digital surveillance industry regularly compromise the interests of third-party companies and consumers. The business model of surveillance companies relies on the ongoing discovery and exploitation of vulnerabilities in widely-used third-party digital operating systems, such as iOS and Windows, and applications such as WhatsApp, etc. Surveillance companies' profit thus depends on actively undermining the products of and ultimately generating costs to other technology manufacturers, with the end result that users of those technologies are less secure. In some cases surveillance companies may also incorporate legitimate companies' hosting or communications services as part of the spyware's operational infrastructure (for purposes of obfuscation or social engineering).[22] In such cases the surveillance activity might additionally amount to violations of intellectual property law, consumer protection law, and contractual terms of service. Such activity also implicates significant public policy arguments as to who bears the costs and who reaps the benefits of privately-manufactured surveillance tools, as well as the strong public interest in responsible disclosure of vulnerabilities of widely-used platforms.

The lack of transparency in the digital surveillance industry further complicates the picture. The purpose of the industry is the enablement, for profit, of state intelligence and security apparatuses. As such, and with the tacit approval of states, this private industry has long attempted to cloak itself in the secrecy traditionally afforded to the state on intelligence and security issues. Indeed, NSO Group has sought to make itself 'transparency-proof' on numerous aspects of its operations, citing Israeli legal requirements and client confidentiality.[23] Yet, while it may be permissible for states to assert secrecy in cases of legitimate, active investigations, a high presumption in favour of disclosure should apply to information regarding human rights violations.[24] Moreover, "business enterprises within the national security sector... have the responsibility to disclose information in respect of situations, activities, or conduct that may reasonably be expected to have an impact on the enjoyment of human rights."[25] Indeed, there is little basis to assert such secrecy regarding corporate activities with significant human rights impacts that fall outside the scope of the public functions of state actors and are fundamentally private in nature, such as relevant contractual templates, internal due diligence and licensing procedures, research and development, corporate structure, investment and financial flows. On such matters the public arguably has an even *stronger* interest in transparency, given the use of public funds to purchase the company's technology and the need to ensure that private sector actors remain accountable.

Because of the threat that government hacking, as a form of surveillance, poses to individuals' privacy as well as to the security of devices, IT systems and the Internet as a whole, it is a matter of debate if it can ever be compatible with international human rights law. Due to the unique and grave threats presented to privacy and security, Privacy International believes that even where governments conduct surveillance in connection with legitimate activities, such as gathering evidence in a criminal investigation or intelligence, they may never be able to demonstrate that hacking as a form of surveillance is compatible with international human rights law.[26] Amnesty International considers

22. See, for example, B. Marczak et al., "Hacking Team's US Nexus," Citizen Lab, February 28, 2014, https://citizenlab.org/2014/02/hacking-teams-us-nexus/

23. See, for example, Novalpina Capital, *Response to Open Letter to Novalpina Capital on 15 April 2019*, www.amnesty.org/download/Documents/DOC10043620 19ENGLISH.PDF

24. See The Global Principles on National Security and the Right to Information (Tshwane Principles), Principles 1, 9 & 10, www.justiceinitiative.org/uploads/bd50b729-d427-4fbb-8da2-1943ef2a3423/global-principles-national-security-10232013.pdf

25. Tshwane Principles, Principle 1(b). Principle 1(e) further states: "Any assertion by a business enterprise of national security to justify withholding information must be explicitly authorized or confirmed by a public authority tasked with protecting national security. *Note: The government, and only the government, bears ultimate responsibility for national security, and thus only the government may assert that information must not be released if it would harm national security.*"

26. Privacy International, Government Hacking and Surveillance: 10 Necessary Safeguards, https://privacyinternational.org/demand/government-hacking-safeguards

that state hacking constitutes a serious interference with human rights, including the right to privacy, and as such it can only be justified under international human rights law in a limited and narrow set of circumstances. SOMO sees the private surveillance industry's business model operating in an unprecedented vacuum outside of public scrutiny, contradicting and undermining international human rights laws and standards, and state hacking through this industry incentivizes profit-driven surveillance companies to normalize and monetize human rights abuse under the guise of national secrecy and national security.

NSO Group has become an important case study on the immense and adverse impact on human rights that digital surveillance companies have, including on the rights to privacy, freedom of opinion and expression, and freedom of association. NSO Group's operations take place from within a complex network of entities – from investors, states, financial organisations and other technology companies – all of whom have contributed to the success of normalizing how this industry operates, with little acknowledgement of the human rights and legal risks endemic to the industry.

4.2 HUMAN RIGHTS LAW APPLICABLE TO STATES AND COMPANIES

Several actors bear human rights responsibilities and obligations regarding the use of government hacking as a form of surveillance, including its development, export and use. States are obliged to have in place adequate legal safeguards to prevent violations by their agents, and also to protect against adverse human rights impacts by companies seeking to export or sell surveillance tools that pose risks to human rights. Surveillance companies like NSO Group, private equity firms that invest in them such as Francisco Partners and Novalpina Capital, and other investors in such companies have a responsibility to respect human rights, avoid causing or contributing to adverse human rights impact through their operations and products, and seek to prevent and mitigate adverse impacts to which they are linked through their business relationships.[27]

States have a duty to protect human rights. Unlawful surveillance violates the right to privacy and can also violate the rights to freedom of expression, opinion, association and peaceful assembly, among others. Both the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) protect these rights. The ICCPR upholds the right to hold opinions without interference[28] and guards against arbitrary and unlawful intrusion on privacy.[29] The targeting of HRDs with digital surveillance technology solely because of their human rights work is unambiguously unlawful under international human rights law.[30] International law and standards also require that any interference by the state on the right to privacy should be lawful, necessary, proportionate and legitimate. States are further required to ensure that individuals whose rights have been violated have access to remedy.[31]

27. Guiding Principles on Business and Human Rights, www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf
28. Article 19, International Covenant on Civil and Political Rights.
29. Article 17, International Covenant on Civil and Political Rights.
30. UN Human Rights Committee General Comment 34, UN Doc. CCPR/C/GC/34, para. 23, www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf
31. UN Human Rights Committee General Comment 34, UN Doc. CCPR/C/GC/34, www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf

In 2013, following a global consultation with civil society groups, industry and international experts in communications surveillance law, policy and technology, a set of 13 international principles on the application of human rights to communications surveillance was developed, called The Necessary and Proportionate Principles.[32] These principles aim to ensure that laws, policies, and practices related to communications surveillance adhere to international human rights laws and standards and adequately protect individual human rights such as privacy and freedom of expression. The principles affirm that any interference with a person's privacy under international human rights law may only be justified when it is prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued.[33] However, many governments deploy surveillance capabilities in secret and without a clear basis in law. In the few instances where governments seek to place such powers on statutory footing, they often do so without the required safeguards and oversight applicable to surveillance activities under international human rights law.[34]

The Necessary and Proportionate Principles call for any government surveillance to have a legal basis; be conducted with a legitimate aim; be necessary, adequate and proportionate; be authorized by a competent judicial authority; follow due process; notify the user where appropriate; be transparent and have public oversight; maintain integrity of communications systems; and have safeguards for international co-operation and the right to effective remedy.

The UN Guiding Principles on Business and Human Rights (UNGPs) also reiterate the international legal obligations of states with respect to the activities of private companies: "States must protect against human rights abuse within their territory and/or jurisdiction by third parties, including business enterprises. This requires taking appropriate steps to prevent, investigate, punish and redress such abuse through effective policies, legislation, regulations and adjudication".[35]

In addition, states have a duty to set out "clearly the expectation that all business enterprises domiciled in their territory and/or jurisdiction respect human rights throughout their operations".[36] Thus, states have an obligation to ensure that surveillance technology companies domiciled in their jurisdiction respect human rights throughout their global operations, including when operating in other jurisdictions.

The human rights responsibilities of companies are likewise laid out in the UNGPs. The UNGPs apply "to all business enterprises, both transnational and others, regardless of their size, sector, location, ownership and structure."[37] They reflect that the private sector has an independent responsibility to respect human rights. In order to fulfil that responsibility, companies must "[a]void causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur," as well as "[s]eek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts."[38] They should do so by carrying out due diligence, a process

32. "The International Principles on the Application of Human Rights to Communications Surveillance (also known as the "Necessary and Proportionate Principles" or "13 Principles") Coalition", May 2014, https://necessaryandproportionate.org/principles/

33. Article 29, Universal Declaration of Human Rights; Human Rights Committee General Comment 27, UN Doc. CCPR/C/21/Rev.1/Add.9, www.refworld.org/docid/45139c394.html

34. Report of the Special Rapporteur on freedom of opinion and expression, UN Doc. A/HRC/23/40, §VI, www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

35. Guiding Principles on Business and Human Rights, www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

36. Guiding Principles on Business and Human Rights.

37. Guiding Principles on Business and Human Rights, p. 1.

38. Principle 13, Guiding Principles on Business and Human Rights.

of identifying, preventing, mitigating, monitoring and accounting for how businesses address their potential and actual adverse impacts.[39] The UNGPs lay out operational principles for companies that include human rights policy commitments, core elements of due diligence, and remediation mechanisms.[40]

4.3 EXPORT REGULATIONS APPLICABLE TO THE DIGITAL SURVEILLANCE INDUSTRY

Digital surveillance products and services of the type sold by NSO Group – a specialized set of offerings that have also been described as "intrusion as a service"[41] provided by "private-sector offensive actors"[42] – fall within multilateral frameworks of export control, and therefore require a licence from state authorities in order to export. These items are considered 'dual use' in nature, meaning that they can be used for both civilian and military purposes without modifications.[43] Export control laws at the national level impose licensing requirements for dual use items for reasons of national security and foreign policy, including in some instances human rights considerations.[44] As states have the obligation to protect from human rights harm by third parties, export licensing could be, when based on solid human rights criteria, a meaningful instrument to do so.

NSO Group has publicly relied on the fact that its exports are licensed by government agencies as an indication of the lawfulness of its products.[45] However, depending on the national legal framework from which the item will be exported, the licensing process may not assess human rights risks or adequately discharge the state's duty to protect. Indeed, authorities may deprioritize human rights risks if countervailing considerations such as industry growth or perceived geopolitical influence weigh

39. Principle 17, Guiding Principles on Business and Human Rights.

40. Guiding Principles on Business and Human Rights, §II.B.

41. The CyberPeace Institute, "CyberPeace Institute Calls for Accountability of Intrusion as a Service Sector", *Medium.com*, 24 December 2020, https://medium.com/the-cyber-peace-institute/cyberpeace-institute-calls-for-accountability-of-intrusion-as-a-service-sector-c1c5597864c3

42. T. Burt, "Cyber mercenaries don't deserve immunity", *Microsoft Blog*, 21 December 2020, https://blogs.microsoft.com/on-the-issues/2020/12/21/cyber-immunity-nso/

43. See for example, European Commission, *Dual-use trade controls*, 2018, https://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/

44. See, for example, US Department of Commerce Bureau of Industry and Security, *Amendment to Licensing Policy for Items Controlled for Crime Control Reasons*, Federal Register Vol. 85, No. 194, 6 October 2020, www.bis.doc.gov/index.php/documents/regulations-docs/federal-register-notices/federal-register-2020/2638-85-fr-63007/file ("The Bureau of Industry and Security (BIS) is amending the Export Administration Regulations (EAR) by revising, in part, the licensing policy for items controlled for crime control (CC) reasons, which is designed to promote respect for human rights throughout the world. BIS also is amending the EAR to provide that, except for items controlled for short supply reasons, it will consider human rights concerns when reviewing license applications for items controlled for reasons other than CC. This revision is necessary to clarify to the exporting community that licensing decisions are based in part upon U.S. Government assessments of whether items may be used to engage in, or enable violations or abuses of, human rights including those involving censorship, surveillance, detention, or excessive use of force.").

45. See, for example, Declaration of Shalev Hulio In Support of Defendants' Motion to Dismiss, *WhatsApp Inc. v. NSO Group Technologies Limited*, 2 April 2020, paras. 5-9, 12, www.courtlistener.com/docket/16395340/45/11/whatsapp-inc-v-nso-group-technologies-limited/; Statement disseminated by Mercury Public Affairs, LLC, on behalf of Q Cyber Technologies Ltd., NSD/FARA Registration Unit, 2 October 2020, https://efile.fara.gov/docs/6170-Informational-Materials-20201002-729.pdf

in favour of licence approval.[46] As noted by the UN Special Rapporteur on freedom of opinion and expression, the global export control framework and its national implementations in which NSO Group operates are inadequate when it comes to regulating such surveillance technology or accounting for human rights impacts.[47] The result is that while NSO Group's exports are indeed "licenced", they could still present a grave risk to human rights, especially in jurisdictions where the legal framework governing the use of its product is inadequate.

Currently, NSO Group is known to export from Israel and European Union (EU) jurisdictions (see discussion below). NSO Group confirmed in correspondence with the authors of this briefing that "Group entities export products from Israel, Bulgaria, and Cyprus, and their respective export control authorities," which have each at some point "denied Group applications for export licenses."[48] Applicable export control frameworks include the following:

WASSENAAR ARRANGEMENT

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is one of several multilateral export control regimes. Forty-two states participate, including most of the world's largest exporters of dual-use goods, such as Bulgaria, India, Russia, the UK, the US, and numerous other EU member states. Israel, though not a Participating State in the Wassenaar Arrangement, incorporates items designated in the Wassenaar control lists within its own national export control regulations.[49] The Wassenaar Arrangement's explicit aim is to promote transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies and to use export controls as a means to combat terrorism. It is not directed against any state or group of states in particular; it aims at harmonizing the export regimes of all participating states.[50]

The central function of the Wassenaar Arrangement is to develop a list of technologies, munitions and dual-use items with the objective of preventing unauthorized transfers or re-transfers of those items. Dual-use goods and technologies to be controlled are those which are major or key elements for the "indigenous development, production, use or enhancement of military capabilities", not because they present human rights risks.[51] The list is negotiated among working groups and updated annually. In 2013, "[s]ystems, equipment, and components therefor, specially designed or modified for the generation, operation or delivery of, or communication with, 'intrusion software'" were added to the

46. See for example, D. Moßbrucker, "EU states unanimously vote against stricter export controls for surveillance equipment", *Netzpolitik.org*, 16 July 2019, https://netzpolitik.org/2019/eu-states-unanimously-vote-against-stricter-export-controls-for-surveillence-equipment/; D. Moßbrucker, "Surveillance exports: How EU Member States are compromising new human rights standards", *Netzpolitik.org,* 29 October 2018, https://netzpolitik.org/2018/surveillance-exports-how-eu-member-states-are-compromising-new-human-rights-standards/; P.H. O'Neill, "Inside NSO, Israel's billion-dollar spyware giant", *MIT Technology Review*, 19 August 2020, www.technologyreview.com/2020/08/19/1006458/nso-spyware-controversy-pegasus-human-rights/ ("In addition, NSO does its own due diligence, says Sunray: its staff examine a country, look at its human rights record, and scrutinize its relationship with Israel. They assess the specific agency's track record on corruption, safety, finance, and abuse – as well as factoring in how much it needs the tool. Sometimes negatives are weighed against positives. Morocco, for example, has a worsening human rights record but a lengthy history of cooperating with Israel and the West on security, as well as a genuine terrorism problem, so a sale was reportedly approved. By contrast, NSO has said that China, Russia, Iran, Cuba, North Korea, Qatar, and Turkey are among 21 nations that will never be customers. Finally, before a sale is made, NSO's governance, risk, and compliance committee has to sign off. The company says the committee, made up of managers and shareholders, can decline sales or add conditions, such as technological restrictions, that are decided case by case."); M. Srivastava & R. Smith, "Israel's NSO: the business of spying on your iPhone," *Financial Times*, 14 May 2019, www.ft.com/content/7f2f39b2-733e-11e9-bf5c-6eeb837566c5

47. Report of the Special Rapporteur on freedom of opinion and expression, UN Doc. A/HCR/41/35, §III.C, www.undocs.org/A/HRC/41/35

48. NSO Group Technologies Ltd. Response to Amnesty International, Privacy International, and SOMO letter, 2 May 2021, at Annex 4. NSO Group also noted, "NSO Group Technologies Ltd., Q Cyber Technologies Ltd., Convexum, Wayout, and the Bulgarian companies export products and obtain licenses from their relevant export authorities for all of the products that require export licenses."

49. Chapter B, Defense Export Control Law 5766-2007 (Unofficial Translation), http://bitly.ws/dA72; D. Hindin, "Can Export Controls Tame Cyber Technology?: An Israeli Approach", *Lawfare*, 12 February 2016, www.lawfareblog.com/can-export-controls-tame-cyber-technology-israeli-approach

50. See Wassenaar Arrangement, www.wassenaar.org

51. Wassenaar Agreement, *Criteria for the Selection of Dual-Use Items*, 2005, www.wassenaar.org/app/uploads/2019/consolidated/08Criteria-for-the-Selection-of-Dual-Use-Goods-including-Sensitive-and-Very-Sensitive-Items.pdf

list,[52] aimed at controlling "surveillance and law enforcement/intelligence gathering tools."[53] This addition in 2013 meant that participating states agreed to require exporters within their jurisdiction to seek a licence prior to any export, and includes products such as NSO Group's Pegasus surveillance tool. In the years since, the participating states have continued to refine and update controls relevant to digital surveillance. The 2020 version of the control list covers "[s]ystems, equipment, and components therefor, specially designed or modified for the generation, command and control, or delivery of 'intrusion software.'"[54]

The Arrangement's mandate, however, does not include the protection of human rights. Rather, its aim is:

> **"to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilising accumulations. Participating States will seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities."[55]**

The Wassenaar Arrangement is not a treaty; it represents a political commitment by its Participating States and rests on voluntary undertakings. States commit to implement additions to the Wassenaar control lists within their domestic regulations.

Therefore, while Wassenaar Arrangement participating states have agreed to require that exporters seek a licence prior to exporting products such as the ones manufactured by NSO Group, the aim is not to protect human rights, but rather to prohibit access by terrorist groups or governments whereby an export would lead to a "destabilising accumulation". States must instead decide, at a national level, the criteria on which basis they shall refuse or grant an export licence. In light of this limitation, the UN Special Rapporteur on freedom of opinion and expression recommended that the Wassenaar states "develop a framework by which the licensing of any [controlled] technology would be conditional upon a national human rights review and companies' compliance with the Guiding Principles on Business and Human Rights," for example through the creation of a human rights working group. He also recommended that the Wassenaar Arrangement "set clear and enforceable guidelines on transparency and accountability with respect to licensing decisions, surveillance-related human rights abuses and the treatment of digital vulnerabilities."[56]

EUROPEAN UNION DUAL-USE REGULATION

Jurisdictions within the EU administer export controls based on the Council Regulation (EC) No 428/2009[57] – a recast of which was adopted in March 2021 – which regulates and partly harmonizes

52. Wassenaar Arrangement, List of Dual-Use Goods and Technologies and Munitions List, 4 December 2013, at 4.A.5. www.wassenaar.org/app/uploads/2019/consolidated/WA-LIST%20%2813%29%201.pdf

53. Wassenaar Arrangement, *Background Documents and Plenary-related and Other Statements*, 2019, p. 47, www.wassenaar.org/app/uploads/2019/12/WA-DOC-19-PUB-006-Public-Docs-Vol-IV-Background-Docs-and-Plenary-related-and-other-Statements-Dec.-2019.pdf

54. Wassenaar Arrangement, *List of Dual-Use Goods and Technologies and Munitions List*, December 2020, at 4.A.5. www.wassenaar.org/app/uploads/2020/12/Public-Docs-Vol-II-2020-List-of-DU-Goods-and-Technologies-and-Munitions-List-Dec-20-3.pdf

55. Wassenaar Arrangement, *Founding Documents*, 2019, www.wassenaar.org/app/uploads/2019/12/WA-DOC-19-Public-Docs-Vol-I-Founding-Documents.pdf

56. Report of the Special Rapporteur on freedom of opinion and expression, UN Doc. A/HCR/41/35, Para 66(f), www.undocs.org/A/HRC/41/35

57. Council of the European Union, Council Regulation (EC) No 428/2009 of 5 May 2009: setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, 2009, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:134:0001:0269:en:PDF

EU member states' controls on dual-use items, and itself incorporates the control lists of the Wassenaar Arrangement (the "Dual-Use Regulation"). Once changes are made to the control lists of the Wassenaar Arrangement, the Dual-Use Regulation is amended to update the common EU control list, which is then applicable across member states.[58] Accordingly, the same items related to "intrusion software" and other surveillance tools designated in the aforementioned Wassenaar Arrangement updates were also incorporated in EU export controls.[59] These export controls are implemented by the EU member states, which may additionally "prohibit or impose an authorisation requirement on the export of dual-use items not listed in [the common control list] for reasons of public security or human rights considerations."[60] A competent authority of each member state decides on the license requests from companies.

Novalpina Capital stated in March 2019 that "[s]ome 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."[61] In correspondence with the authors of this briefing, NSO Group confirmed that group entities sought export licenses from Bulgaria and Cyprus.[62]

The national processes by which EU member states assess export licences vary, and in practice have not prevented export of surveillance technologies to states known to use them in violation of international human rights law.[63] For the export of the type of products manufactured by NSO Group to countries outside the EU an export license must be obtained.[64] In the authorization process of such a license the competent authority of the member state must take into account Article 12 of the Dual-Use Regulation. That provision states that: "In deciding whether or not to grant [an export licence], the Member States shall take into account… considerations of national foreign and security policy, including those covered by Council Common Position 2008/944/CFSP of 8 December 2008 defining common rules governing control of exports of military technology and equipment." Council Common Position 2008/944/CFSP, defining common rules governing the control of exports of military technology and equipment, is a legally binding agreement that outlines eight criteria against which export authorities must assess licence applications, including the threat to regional peace and security and taking into account international embargos. Criterion Two of the Common Position, "Respect for human rights in the country of final destination as well as respect by that country of international humanitarian law" indicates that member states shall "deny an export licence if there is a clear risk that the military technology or equipment to be exported might be used for internal repression."[65]

---

58. The EU control list updated as of December 2020 is available at https://trade.ec.europa.eu/doclib/docs/2020/december/tradoc_159198.pdf

59. See category 4A005, 4D004 and 4E004C of Annex I juncto art. 3 Regulation (EC) No 428/2009 (consolidated version).

60. Article 8(1), EU Council Regulation (EC) No 428/2009.

61. Novalpina Capital, *Response to Open Letter to Novalpina Capital on 18 February 2019*, www.amnesty.org/download/Documents/DOC10021020 19ENGLISH.PDF; see also L. Krahulcova, "Is NSO Group's infamous Pegasus spyware being traded through the EU?", *Access Now,* 12 September 2019, www.accessnow.org/is-nso-groups-infamous-pegasus-spyware-being-traded-through-the-eu/

62. NSO Group Technologies Ltd. Response to Amnesty International, Privacy International, and SOMO letter, 2 May 2021, at Annex 4.

63. See European Commission, Commission Staff Working Document Impact Assessment. Report on the EU Export Control Policy Review, 28 September 2016, para. 1.2.1.2 and Chapter 2, https://trade.ec.europa.eu/doclib/docs/2016/october/tradoc_155008.pdf; Amnesty International, *Out of control: Failing EU laws for digital surveillance export* (Index: EUR 01/2556/2020), www.amnesty.org/download/Documents/EUR0125562020ENGLISH.PDF; Human Rights Watch, "EU: Strengthen Rules on Surveillance Tech Exports," 9 June 2020, https://www.hrw.org/news/2020/06/09/eu-strengthen-rules-surveillance-tech-exports; L. Krahulcova, "Case study: Denmark and the failure of EU export controls," *Access Now*, 6 September 2017, www.accessnow.org/case-study-denmark-failure-eu-export-controls/. See also L. Krahulcova, "New report: FinFisher changes tactics to hook critics," *Access Now*, 14 May 2018, www.accessnow.org/new-report-finfisher-changes-tactics-to-hook-critics/; Amnesty International, "German-made FinSpy spyware found in Egypt, and Mac and Linux versions revealed," 25 September. 2020, www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/; and C. Cimpanu, "New versions of FinFisher mobile spyware discovered in Myanmar," ZDNet, 10 July 2019, www.zdnet.com/article/new-versions-of-finfisher-mobile-spyware-discovered-in-myanmar/.

64. Art. 3(1) juncto category 4A005, 4D004 and 4E004C of Annex I Regulation (EC) No 428/2009 (consolidated version).

65. Council of the European Union, Council Common Position 2008/944/CFSP of 8 December 2008 defining common rules governing control of exports of military technology and equipment, 2008, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008E0944

At present, however, both the Dual-Use Regulation and the Common Position are poorly implemented by member state export authorities when authorizing exports of surveillance equipment and do not provide sufficient detail regarding the assessment of the potential human rights risks posed by importing states. Through the Coalition Against Unlawful Surveillance Exports (CAUSE), Amnesty International, Access Now, Human Rights Watch, Privacy International, and other NGOs have for many years called for reforms to the Dual-Use Regulation to ensure that strong criteria exist that clearly stipulate which considerations should be applied when assessing export licence applications for surveillance technology.[66] For example, the current EU legislation lacks requirements for competent authorities of member states to assess the adequacy of the legal framework as it relates to the use of surveillance technology in the country of destination; indeed, there is no need to even consider if the end-use of the technology by the end-user is lawful in the importing jurisdiction. As a consequence, export authorities of EU member states have approved the vast majority of export licence applications for surveillance technology. Research by Security for Sale indicates that EU member states permitted exports of surveillance technology at least 317 times between 2015-2017, while denying only 14 applications.[67] A February 2021 report of the European Commission noted that in 2018, 131 licenses and 27 denials were issued for cyber-surveillance items.[68]

In light of the many developments concerning dual-use technology and the human rights impacts of surveillance and other exports, the EU has been working to recast the Dual-Use Regulation since 2016.[69] The European Parliament and EU Council adopted a new regulation in March 2021, which, although intended to address human rights concerns, reflected a number of concessions to industry and governments that left key human rights-related provisions watered down.[70] The compromise text,[71] agreed upon in November 2020, now includes "cyber-surveillance items" as a special category of dual-use items. With the new text of the Regulation, the function of EU surveillance export law has changed from being an instrument purely for surveillance export controls by regulating primarily the export of items that have been placed on the control list, to an instrument of export regulation that also lays down obligations and responsibilities for exporters of cyber-surveillance technologies that are not (yet) placed on the control list. For example, it revises the catch-all provision to require licence authorization for the export of non-listed cyber-surveillance technologies that "are or may be intended... for use in connection with internal repression and/or the commission of serious violations of international human

66. CAUSE, *A critical opportunity: bringing surveillance technologies within the EU Dual-Use Regulation*, 2015, https://www.fidh.org/IMG/pdf/cause_report_final.pdf Access Now, "Human rights organizations call to strengthen the European Commission position on dual-use recast," 9 June 2020, www.accessnow.org/human-rights-organizations-call-to-strengthen-the-european-commission-position-on-dual-use-recast/; Amnesty International, *Urgent call to the Council of the EU: Human Rights must come first in Dual Use final draft*, 9 November 2020, www.amnesty.eu/news/urgent-call-to-the-council-of-the-eu-human-rights-must-come-first-in-dual-use-final-draft/

67. S. Gjerding & L. Skou Andersen, "How European spy technology falls into the wrong hands", *De Correspondent*, 23 February 2017, https://thecorrespondent.com/6257/how-european-spy-technology-falls-into-the-wrong-hands/2168866237604-51234153

68. European Commission, *Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EC) No 428/2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items*, COM(2021) 42 final, 3 February 2021, https://ec.europa.eu/transparency/regdoc/rep/1/2021/EN/COM-2021-42-F1-EN-MAIN-PART-1.PDF, at p. 4.

69. B. Immenkamp, *Briefing: EU Legislation in Progress: Review of Dual-Use Export Controls*, European Parliamentary Research Service, 2021, www.europarl.europa.eu/RegData/etudes/BRIE/2016/589832/EPRS_BRI(2016)589832_EN.pdf

70. Access Now et al., "New EU Dual Use Regulation agreement 'a missed opportunity' to stop exports of surveillance tools to repressive regimes," Amnesty International, 25 March 2021, www.amnesty.org/en/latest/news/2021/03/new-eu-dual-use-regulation-agreement-a-missed-opportunity-to-stop-exports-of-surveillance-tools-to-repressive-regimes/; Amnesty International, *Out of control: Failing EU laws for digital surveillance export* (Index: EUR 01/2556/2020), www.amnesty.org/download/Documents/EUR0125562020ENGLISH.PDF. The recommendations from the Amnesty International report *Out of control* are linked to the provisions in the Recast Dual-Use Regulation in the chart at Access Now, "Urgent call to Council of the EU: human rights must come first in Dual Use final draft," 5 November 2020, www.accessnow.org/urgent-call-to-council-of-the-eu-human-rights-must-come-first-in-dual-use-final-draft/. See also B. Immenkamp, *Briefing: EU Legislation in Progress: Review of Dual-Use Export Controls*, European Parliamentary Research Service, 2021, www.europarl.europa.eu/RegData/etudes/BRIE/2016/589832/EPRS_BRI(2016)589832_EN.pdf

71. Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast) - Confirmation of the final compromise text with a view to agreement,* 12798/20, 13 November 2020, https://data.consilium.europa.eu/doc/document/ST-12798-2020-INIT/en/pdf

rights and international humanitarian law."[72] There are special responsibilities and obligations for exporters to notify the competent authorities of the risks of serious human rights violations associated with their intended exports.[73] It also refers to the due diligence obligations and responsibilities of companies, and lays out additional reporting requirements intended to enhance transparency.[74] It remains to be seen whether the revised Dual-Use Regulation will more effectively curb the spread of EU-supplied surveillance technologies to states using them in violation of human rights.

ISRAEL

Israel regulates the export of certain dual-use technologies on the basis of its Defense Export Control Law 5766, 2007.[75] While Israel is not a Participating State in the Wassenaar Arrangement, it incorporates items designated in the Wassenaar control lists within its own national export control regulations.[76] The objective of the Defense Export Control Law is to "regulate state control of the export of defense equipment, the transfer of defense know-how and the provision of defense services, for reasons of national security considerations, foreign relations considerations, international obligations and other vital interests of the State". Human rights considerations are not mentioned within the law itself and there is no elaboration available on how extensively and appropriately Israel's human rights obligations are considered in making determinations. While the Israeli Ministry of Foreign Affairs may submit a position on an application, it is the Ministry of Defense (MOD) that ultimately approves and denies export applications.[77] Notably, in addition to a licence for export, Israeli corporations must obtain licences for any defence marketing activity – "[a]n activity aimed at promoting a defense export transaction, including brokering activity towards a defense export transaction" – in which they engage.[78] Recent export control reforms intended to streamline the process, however, allow companies to obtain exemptions from the marketing licence for certain sales to specified countries.[79]

The MOD grants one or more entities in the NSO corporate structure export licences to sell their technology overseas. This has been confirmed by Novalpina Capital in a public response to an open letter written by Amnesty International, Privacy International and others, which states: "Export licences are typically (although not exclusively) granted by the Israeli authorities."[80] In May 2019, Novalpina

72. Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast) - Confirmation of the final compromise text with a view to agreement,* 12798/20, 13 November 2020, Art. 4a(1), https://data.consilium.europa.eu/doc/document/ST-12798-2020-INIT/en/pdf

73. Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast) - Confirmation of the final compromise text with a view to agreement,* 12798/20, 13 November 2020, Art. 4a(2), https://data.consilium.europa.eu/doc/document/ST-12798-2020-INIT/en/pdf

74. B. Immenkamp, *Briefing: EU Legislation in Progress: Review of Dual-Use Export Controls*, European Parliamentary Research Service, 2021, www.europarl.europa.eu/RegData/etudes/BRIE/2016/589832/EPRS_BRI(2016)589832_EN.pdf

75. Defense Export Control Law, 5766-2007 (Unofficial Translation), http://bitly.ws/dA72

76. Chapter B, Defense Export Control Law 5766-2007 (Unofficial Translation), http://bitly.ws/dA72; D. Hindin, "Can Export Controls Tame Cyber Technology?: An Israeli Approach", *Lawfare*, 12 February 2016, www.lawfareblog.com/can-export-controls-tame-cyber-technology-israeli-approach

77. Amnesty International, *Novalpina Capital's Reply to NGO Coalition Letter (15 April 2019) and Citizen Lab Letter (06 March 2019)* (Index: DOC 10/0436/2019), www.amnesty.org/en/documents/doc10/0436/2019/en/; see also: D. Hindin, *Regulation of Cyber Tools in Israel: Export Controls, Encryption Licensing and Economic Sanctions,* 2017, p.9, www.americanconference.com/7th-advanced-industry-forum-global-encryption-controls/wp-content/uploads/sites/1741/2017/03/Day2_945am_Hindin.pdf

78. §14, Defence Export Control Law 5766-2007 (Unofficial Translation), http://bitly.ws/dA72

79. T. Cohen & A. Rabinovitch, "Israel eases rules on cyber weapons exports despite criticism", *Reuters*, 22 August 2019, www.reuters.com/article/us-israel-hackers/israel-eases-rules-on-cyber-weapons-exports-despite-criticism-idUSKCN1VC0XQ

80. Novalpina Capital, *Response to Open Letter to Novalpina Capital on 18 February 2019*, https://www.amnesty.org/download/Documents/DOC1002102019ENGLISH.PDF

Capital released a legal opinion on the application of export control regulations in Israel.[81] The opinion confirmed that all of NSO Group's current product line falls within the defence export control regime, meaning it is administered by the Defence Exports Control Agency (DECA), a unit of the MOD, under the 2007 Defence Export Control Law.

Transparency around defence exports in Israel is significantly curtailed. As Novalpina Capital states, there exist "significant constraints on lawful disclosure under the Israeli export licence regime."[82] The aforementioned legal opinion asserts that providing any information to an unauthorized third party without the express written permission and prior authorization of DECA would be a violation of Section 113 of the 1977 Penal Law and could lead to criminal proceedings.[83] The opinion continues by stating:

> **"we are aware of several cases (the details of which we are not at liberty to discuss) in which this DECA license confidentiality requirement was invoked in the context of international investigations and court proceedings, resultantly preventing any disclosure of information relating to defence exports, including details relating to DECA licenses."**

If accurate, this means that with respect to exports from Israel, Novalpina Capital and NSO Group are likely to be unable to comply with Principle 21 of the UNGPs, which indicates that businesses should communicate externally about "how they address their human rights impacts," including through formal reporting, in order to "know and show that they respect human rights in practice."[84] At the same time, the restrictions raise questions regarding Israel's duty to protect: the UNGPs note that states should ensure that laws applicable to business enterprises "do not constrain but enable business respect for human rights," and "[e]ncourage, and where appropriate require, business enterprises to communicate how they address their human rights impacts."[85] The constraints on transparency in Israel as outlined in the legal opinion released by Novalpina Capital are consistent with other analyses, including the 2018 Small Arms Survey Transparency Barometer, which places Israel as among the five least transparent small arms exporters in the world, together with Saudi Arabia, Iran, North Korea, and the United Arab Emirates.[86]

Additionally, there have been other credible reports that Israel's current export licensing regime does not provide appropriate limitations on exports when there is a high probability that they will be used in violation of human rights.[87] And further, in an administrative action for revocation of the export licence granted to NSO Group, brought by petitioners in Israel and supported by Amnesty International, relief was denied by the Tel Aviv District Court in spite of evidence that NSO technology was used to target an Amnesty International staff member and other human rights defenders (see Section 5 below).[88]

---

81. Novalpina Capital, *Response to Open Letter to Novalpina Capital on 15 April 2019*, www.amnesty.org/download/Documents/DOC1004362019ENGLISH.PDF

82. Novalpina Capital, *Response to Open Letter to Novalpina Capital on 15 April 2019.*

83. Novalpina Capital, *Response to Open Letter to Novalpina Capital on 15 April 2019.*

84. Guiding Principles on Business and Human Rights, www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

85. Principle 3, Guiding Principles on Business and Human Rights.

86. P. Holtom & I. Pavesi, *The 2018 Small Arms Trade Transparency Barometer*, 2018, www.smallarmssurvey.org/fileadmin/docs/T-Briefing-Papers/SAS-BP-Transparency-Barometer-2018.pdf

87. R. Silverstein, "Israel's Genocidal Arms Customers", *Jacobin*, (n.d.), https://jacobinmag.com/2018/11/israel-arms-sales-eitay-mack-idf; A. Harel, "Arming Dictators, Equipping Pariahs: Alarming Picture of Israel's Arms Sales", *Haaretz*, 19 May 2019, www.haaretz.com/israel-news/.premium-israel-arms-sales-to-dictators-pariahs-states-alarming-picture-1.7250048; Associated Press, "Israel's role in South Sudan under scrutiny", *Ynetnews.com*, 9 October 2016, https://www.ynetnews.com/articles/0,7340,L-4852711,00.html; A. Pick, "Up in Arms about Israeli Arms Exports", CTech by Calcalist, 15 February 2019, www.calcalistech.com/ctech/articles/0,7340,L-3756398,00.html

88. Amnesty International, *Israel: Court rejects bid to revoke notorious spyware firm NSO Group's export licence* (News story, 12 July 2020), www.amnesty.org/en/latest/news/2020/07/israel-court-notorious-spyware-firm-nso/

In sum, international and regional export control regimes, as well as export regulations in place in Israel, currently fail to adequately protect human rights. Export authorities have licensed surveillance items such as those manufactured by NSO Group for export to countries with track records of surveillance and human rights abuses, demonstrating that potential human rights impacts are not determinative in licence decisions. The Israeli MOD's record of approving export licences despite the risk that surveillance technology could be used for human rights violations shows that strategic considerations outweigh human rights concerns, while secrecy provisions undermine NSO Group's ability to meet its own human rights responsibilities. While other jurisdictions from which NSO Group exports, such as the EU (Bulgaria and Cyprus), have the legal basis to include human rights criteria in their assessments, reporting suggests that in general human rights considerations are not decisive criteria in those licensing decisions (albeit complete information about destination countries and products is unavailable).[89]

89. See for example, S. Gjerding & L. Skou Andersen, "How European Spy Technology Falls into the Wrong Hands", *De Correspondent*, 23 February 2017, https://thecorrespondent.com/6257/how-european-spy-technology-falls-into-the-wrong- hands/2168866237604-51234153

5. MOUNTING EVIDENCE OF SURVEILLANCE ABUSES INVOLVING NSO GROUP TECHNOLOGY

Researchers, journalists, activists and others have uncovered significant evidence over the years of the use of NSO Group's surveillance technology to target individuals around the world in violation of their internationally recognized human rights. While NSO Group asserts that its government clients are contractually obligated to use its products only for "the prevention and investigation of serious crimes, including terrorism, and to ensure that the products will not be used to violate human rights,"[90] the track record of deployment suggests a broad parallel use to surveil civil society. For example, documented targets of surveillance reliant on NSO Group technology include:

- Ahmed Mansoor,[91] a human rights defender in the United Arab Emirates, who was targeted with NSO Group technology in 2016. He was arrested in March 2017 and remains imprisoned in solitary confinement without access to medication or other necessities.[92]
- A scientist and two public health advocates working to support a soda tax in Mexico.[93]
- Journalists and organizations in Mexico working on issues related to corruption, including television personality and investigative journalist Carmen Aristegui and her son, who was a minor at the time.[94]
- Journalists at *Río Doce* newspaper investigating organized crime and cartels in Mexico, the

90. NSO Group Human Rights Policy

91. B. Marczak & J. Scott-Railton, "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender", Citizen Lab, 24 August 2016, https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

92. Human Rights Watch, *UAE: Imprisoned Activist's Health at Risk,* 16 December 2020, www.hrw.org/news/2020/12/16/uae-imprisoned-activists-health-risk

93. J. Scott-Railton et al., "Bitter Sweet: Supporters of Mexico's Soda Tax Targeted with NSO Exploit Links", *Citizen Lab,* 11 February 2017, https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/

94. J. Scott-Railton et al., "Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware", *Citizen Lab,* 19 June 2017, https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/; J. Scott-Railton et al., "Reckless V: Director of Mexican Anti-Corruption Group Targeted with NSO Group's Spyware", *Citizen Lab,* 30 August 2017, https://citizenlab.ca/2017/08/nso-spyware-mexico-corruption/

targeting of whom took place in the wake of the murder of *Río Doce's* co-founder;[95] as well as the wife of their slain colleague, herself a journalist.[96]

- Lawyers[97] and a journalist[98] whose work concerned the investigation of murders potentially linked to state and federal authorities in Mexico.
- International expert investigators working on the 2014 Iguala Mass Disappearance in Mexico, and lawyers working with the families of students disappeared in that incident.[99]
- Politicians, including a senator, who were members of the conservative National Action Party (PAN) in Mexico.[100]
- Omar Abdulaziz, a Saudi activist and permanent resident of Canada. Omar Abdulaziz was also a close colleague of murdered Saudi journalist and dissident Jamal Khashoggi, with whom he had been in regular contact on his mobile device.[101]
- An Amnesty International staff member, who received a suspicious link in June 2018 baited with Saudi Arabia-related content that, if opened, would have deployed potent spyware. Through the course of subsequent investigations, Amnesty International discovered that a Saudi Arabian activist based abroad, Yahya Assiri, had also received similar malicious messages.[102] Amnesty International determined that NSO Group's Pegasus spyware was used against the two targets.[103]
- Maati Monjib, an academic and activist working on freedom of expression, and Abdessadak El Bouchattaoui, a human rights lawyer, both from Morocco.[104] Targeted attacks against these individuals, dating back to at least 2017, were carried out through SMS messages carrying malicious links that, if clicked, would attempt to exploit the mobile device of the victim and install NSO Group's Pegasus spyware. In addition to SMS messages, Amnesty International identified network injection attacks against Maati Monjib also aimed at installing spyware. Amnesty International suspects that NSO Group technology may have been used in these network injection attacks as well.[105]

---

95. J. Scott-Railton et al., "Reckless VI: Mexican Journalists Investigating Cartels Targeted with NSO Spyware Following Assassination of Colleague", *Citizen Lab*, 27 November 2018, https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/

96. J. Scott-Railton et al., "Reckless VII: Wife of Journalist Slain in Cartel-Linked Killing Targeted with NSO Group's Spyware", *Citizen Lab*, 20 March 2019, https://citizenlab.ca/2019/03/nso-spyware-slain-journalists-wife/

97. J. Scott-Railton et al., "Reckless IV: Lawyers for Murdered Mexican Women's Families Targeted with NSO Spyware", *Citizen Lab*, 2 August 2017, https://citizenlab.ca/2017/08/lawyers-murdered-women-nso-group/

98. J. Scott-Railton et al., "Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware", *Citizen Lab*, 19 June 2017, https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/

99. J. Scott-Railton et al., "Reckless III: Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware", *Citizen Lab*, 10 July 2017, https://citizenlab.ca/2017/07/mexico-disappearances-nso/; J. Scott-Railton et al., "Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware", *Citizen Lab*, 19 June 2017, https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/

100. J. Scott-Railton et al., "Reckless Redux: Senior Mexican Legislators and Politicians Targeted with NSO Spyware", *Citizen Lab*, 29 June 2017, https://citizenlab.ca/2017/06/more-mexican-nso-targets/

101. B. Marczak et al., "The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil" *Citizen Lab*, 1 October 2018, https://citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soi; K. Shaheen, "'They silenced Khashoggi but gave thousands a voice'", *The Guardian*, 24 November 2018, https://www.theguardian.com/world/2018/nov/24/jamal-khashoggi-omar-abdulaziz-dissident-saudis-interview

102. T. Brewster,"Exclusive: Saudi Dissidents Hit With Stealth iPhone Spyware Before Khashoggi's Murder," *Forbes*, 21 November 2018, www.forbes.com/sites/thomasbrewster/2018/11/21/exclusive-saudi-dissidents-hit-with-stealth-iphone-spyware-before-khashoggis-murder/

103. Amnesty International, *Amnesty International among Targets of NSO-powered Campaign* (News story, 1 August 2018), https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/

104. Amnesty International, *Morocco: Human Rights Defenders Targeted with NSO Group's Spyware* (Blog, 10 October 2019), www.amnesty.org/en/latest/research/2019/10/morocco-human-rights-defenders-targeted-with-nso-groups-spyware/

105. See: Amnesty International, *Morocco: Human Rights Defenders Targeted with NSO Group's Spyware* (Blog, 10 October 2019), www.amnesty.org/en/latest/research/2019/10/morocco-human-rights-defenders-targeted-with-nso-groups-spyware/

- A lawyer in the UK involved in a civil action filed against NSO Group.[106]
- A journalist from the US reporting on Saudia Arabia, who is based in Lebanon.[107]
- A Catalan politician and pro-independence supporters in Spain.[108]
- Over 1,400 individuals targeted with an NSO Group exploit of Facebook's WhatsApp platform, disclosed by WhatsApp in October 2019.[109] WhatsApp, in collaboration with Citizen Lab, revealed that more than 100 of these targets were HRDs, activists and journalists, across numerous countries including Bahrain, the United Arab Emirates and Mexico.[110] Subsequent media reporting revealed that the targets included Rwandan political dissidents living abroad,[111] and activists and HRDs from India[112] and Morocco.[113] Facebook and WhatsApp sued NSO Group in the US over this use of WhatsApp to deliver spyware.[114] A number of NGOs, including Access Now, Amnesty International and Privacy International, filed an amicus brief[115] in the action that also detailed the targeting via the NSO WhatsApp exploit of the following individuals: Bela Bhatia, a human rights lawyer and activist in India; Aboubakr Jamaï, a journalist in Morocco; Fouad Abdelmoumni, a HRD in Morocco; Placide Kayumba, an activist in Rwanda; and Father Pierre Marie-Chanel Affognon, a Catholic priest and founder of a reform movement in Togo.[116] The suit is still pending.

Given the secrecy associated with targeted digital surveillance, and NSO Group's strong resistance to providing any details of its sales or efforts to prevent and address misuse of its technology, this record likely represents just a small window into a much larger phenomenon.

The documentation of NSO Group's involvement in targeted surveillance against human rights defenders and other civil society actors has resulted in significant legal exposure of the company, including active litigation in Israel, Cyprus and the US.[117] Notably, the WhatsApp case filed against NSO Group and Q Cyber Technologies in the US generated substantial amicus participation in support of

---

106. N. Hopkins & D. Sabbagh, "WhatsApp spyware attack was attempt to hack human rights data, says lawyer", *The Guardian*, 14 May 2019, www.theguardian.com/technology/2019/may/14/whatsapp-spyware-vulnerability-targeted-lawyer-says-attempt-was-desperate

107. B. Marczak et al., "Stopping the Press: New York Times Journalist Targeted by Saudi-linked Pegasus Spyware Operator", *Citizen Lab*, 28 January 2020, https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/

108. S. Kirchgaessner & S. Jones, "Phone of top Catalan politician 'targeted by government-grade spyware'", *The Guardian*, 13 July 2020, www.theguardian.com/world/2020/jul/13/phone-of-top-catalan-politician-targeted-by-government-grade-spyware

109. W. Cathcart, "Opinion: Why WhatsApp is pushing back on NSO Group hacking", *Washington Post*, 29 October 2019, www.washingtonpost.com/opinions/2019/10/29/why-whatsapp-is-pushing-back-nso-group-hacking/

110. Citizen Lab, "NSO Group / Q Cyber Technologies: Over One Hundred New Abuse Cases," *Citizen Lab*, 29 October 2019, https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/

111. See M. Srivastava and T. Wilson, "Inside the WhatsApp hack: how an Israeli technology was used to spy," *Financial Times*, 29 October 2019, www.ft.com/content/d9127eae-f99d-11e9-98fd-4d6c20050229; C. Bing & R. Satter, "Exclusive: Government officials around the globe targeted for hacking through WhatsApp – sources", Reuters, 31 October 2019, www.reuters.com/article/us-facebook-cyber-whatsapp-nsogroup/exclusive-whatsapp-hacked-to-spy-on-top-government-officials-at-u-s-allies-sources-idUSKBN1XA27H

112. Scroll, "WhatsApp spyware: 22 confirmed cases of activists, lawyers, scholars targeted in India", *Scroll.in*, 31 October 2019, https://scroll.in/latest/942218/nagpur-lawyer-notified-by-whatsapp-of-surveillance-says-bhima-koregaon-accused-were-also-targetted

113. See S. Kirchgaessner et al., "WhatsApp 'hack' is serious rights violation, say alleged victims", *The Guardian*, 1 November 2019, www.theguardian.com/technology/2019/nov/01/whatsapp-hack-is-serious-rights-violation-say-alleged-victims

114. W. Cathcart, "Opinion: Why WhatsApp is pushing back on NSO Group hacking", *Washington Post*, 29 October 2019, www.washingtonpost.com/opinions/2019/10/29/why-whatsapp-is-pushing-back-nso-group-hacking/; Docket Entries, *WhatsApp Inc. v. NSO Group Technologies Limited* (4:19-cv-07123), District Court, N.D. California, www.courtlistener.com/docket/16395340/whatsapp-inc-v-nso-group-technologies-limited/

115. Access Now et al., *Amicus Brief in WhatsApp Inc. v. NSO Group Technologies Limited*, 2020, https://www.accessnow.org/cms/assets/uploads/2020/12/2020-12-22-AccessNow-Amicus-Brief13845453.1.pdf

116. Access Now, *From India to Rwanda, the victims of NSO Group's WhatsApp hacking speak out*, 17 December 2020, https://www.accessnow.org/nso-whatsapp-hacking-victims-stories/

117. S. Anstis, "NSO Group", *Citizen Lab*, 12 December 2018, https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/#NSO

the argument that NSO Group is not entitled to immunity from suit. They included civil society groups (Access Now, Amnesty International, Committee to Protect Journalists, Internet Freedom Foundation, Paradigm Initiative, Privacy International, Reporters Without Borders, Red en Defensa de los Derechos Digitales [R3D],[118] as well as Electronic Frontier Foundation[119]), individual experts (former UN Special Rapporteur on freedom of opinion and expression David Kaye,[120] and three foreign sovereign immunity scholars[121]), and global technology companies (Microsoft, Cisco, GitHub, Google, LinkedIn, VMWare, and the Internet Association on behalf of its members).[122] As a statement from Microsoft explained in connection with the company's participation as amicus in the *WhatsApp v. NSO Group* lawsuit:

> **"We believe the NSO Group's business model is dangerous.... First, [private-sector offensive actors'] presence increases the risk that the weapons they create fall into the wrong hands.... Second, private-sector companies creating these weapons are not subject to the same constraints as governments.... Third, companies like the NSO Group threaten human rights whether they seek to or not."[123]**

Additionally, petitioners in Israel brought an administrative action in 2019, supported by Amnesty International, to require the Israeli Ministry of Defense to revoke the export licence of NSO Group in connection with the targeting of the Amnesty International staff member.[124] While the case was heard under a gag order[125] and the court ultimately declined to order revocation of the export licence,[126] it is an example of a public challenge to the authorization of NSO Group exports that may continue to emerge.

118. Access Now et al., *Amicus Brief in WhatsApp Inc. v. NSO Group Technologies Limited,* 2020, www.accessnow.org/cms/assets/uploads/2020/12/2020-12-22-AccessNow-Amicus-Brief13845453.1.pdf

119. Electronic Frontier Foundation, *Amicus Brief in WhatsApp Inc. v. NSO Group Technologies Limited,* 2020, www.eff.org/document/eff-amicus-brief-whatsapp-v-nso-group-9th-cir

120. D. Kaye, *Amicus Brief in WhatsApp Inc. v. NSO Group Technologies Limited,* 2020, www.accessnow.org/cms/assets/uploads/2021/01/Amicus-Special-Rapporteur.pdf

121. Foreign Sovereignty Immunity Scholars, *Amicus Brief in WhatsApp Inc. v. NSO Group Technologies Limited*, 2020, www.accessnow.org/cms/assets/uploads/2021/01/2020-12-23-Foreign-Sovereign-Immunity-Scholars-Amicus-Brief.pdf

122. Microsoft Corp. et al., *Amicus Brief in WhatsApp Inc. v. NSO Group Technologies Limited,* 2020, https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2020/12/NSO-v.-WhatsApp-Amicus-Brief-Microsoft-et-al.-as-filed.pdf

123. T. Burt, "Cyber mercenaries don't deserve immunity", *Microsoft Blog*, 21 December 2020, https://blogs.microsoft.com/on-the-issues/2020/12/21/cyber-immunity-nso/

124. Amnesty International, *Israel: Amnesty International engages in legal action to stop NSO Group's web of surveillance* (News story, 13 May 2019), www.amnesty.org/en/latest/news/2019/05/israel-amnesty-legal-action-stop-nso-group-web-of-surveillance/

125. Amnesty International, *Israel: Court decides to hear case against NSO behind closed doors* (News story, 16 January 2020), www.amnesty.org/en/latest/news/2020/01/israel-court-nso-case-behind-closed-doors/

126. Amnesty International, *Israel: Court rejects bid to revoke notorious spyware firm NSO Group's export licence* (News story, 12 July 2020), www.amnesty.org/en/latest/news/2020/07/israel-court-notorious-spyware-firm-nso/

6. THE NSO CORPORATE STRUCTURE

As NSO Group has expanded its business over time, and its investors and ownership have changed, its corporate structure has likewise evolved. This section outlines and explains the evolution of NSO Group's corporate structure and includes diagrams to aid comprehension, in order to further transparency regarding company ownership, control, and operations. Initial references to the names of particular corporate entities are indicated in bold. The first section explains at a structural level what the NSO Group is, the second details the corporate structure during the Francisco Partners years, and the third looks at the most recent structure after Novalpina Capital's investment.

6.1 WHAT IS "NSO GROUP"?

[See Diagram 1 at page 30.]

Use of the name NSO Group originates with **NSO Group Technologies Ltd.**, an Israeli corporation established on 25 January 2010 (company number 514395409).[127] The founders – the first initials of whom make up the acronym "NSO" – were Israeli businesspersons Niv Carmi,[128] Shalev Hulio and Omri Lavie; an initial investor was venture capitalist Eddy Shalev.[129] According to Shalev Hulio, the goal of the company was to develop technology that would provide law enforcement and intelligence agencies with direct remote access to mobile phones and their content – a workaround to the increasingly widespread use of encryption in the digital environment. Shalev Hulio claimed that the idea was born out of a request from European authorities that were familiar with his and Omri Lavie's existing work on cell phone carrier customer service technology:

> **"'At the time, we knew nothing about this world,' Hulio says. 'And then the police forces and the intelligence agencies of Europe told us: "With the technology you developed, you could help us solve this problem." So us being Israelis and hearing we had technology that could save lives, we immediately said: "Tell us what you need, and we'll do it."'"[130]**

127. Israeli Corporations Authority, Confirmation of incorporation and registration of NSO Group Technologies Ltd., 3 July 2019.

128. NSO Group has confirmed that "Niv Carmi is no longer affiliated with the Group." NSO Group Technologies Ltd. Response to Amnesty International, Privacy International, and SOMO letter, 2 May 2021, at Annex 4.

129. R. Bergman, "Weaving a cyber web", *Ynetnews*, 11 January 2019, https://www.ynetnews.com/articles/0,7340,L-5444998,00.html; S. Schelach, "Francisco Partners buys NSO for $120m", *GlobesOnline*, 19 March 2014, https://en.globes.co.il/en/article-francisco-partners-buys-nso-for-120m-1000925480; F2, Eddy Shalev, (n.d.), www.f2vc.com/f2-team/eddy-shalev

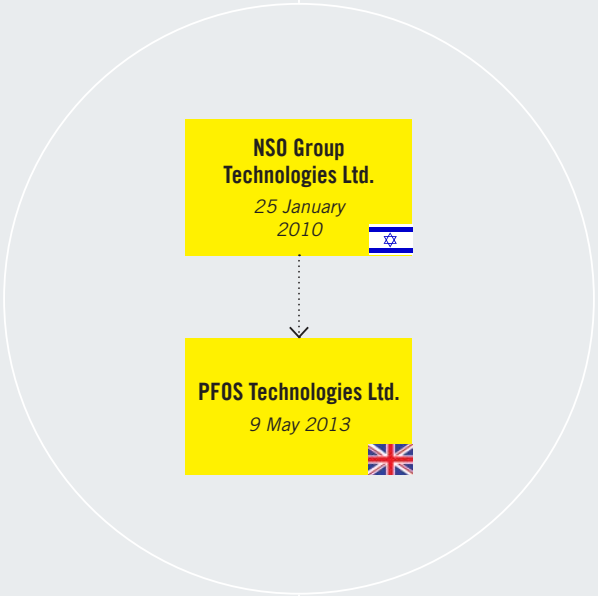
130. R. Bergman, "Weaving a cyber web", *Ynetnews*, 11 January 2019, https://www.ynetnews.com/articles/0,7340,L-5444998,00.html

Diagram 1:

Early years (prior to Francisco Partners)

Registered in Israel

Registered in the UK



Filings in the UK show that NSO Group Technologies Ltd. is the sole shareholder of a UK-based subsidiary called PFOS Technologies Ltd. (incorporated 9 May 2013),[131] the principal activity of which was described as "marketing services for its parent company."[132] Another wholly-owned subsidiary is the Israeli counter-drone company Convexum Ltd., which NSO Group Technologies Ltd. acquired in February 2020 for USD$60 million.[133] One of Convexum's previous shareholders was venture capital firm F2 Capital Ltd.,[134] the chairman of which is NSO Group investor Eddy Shalev.[135] NSO Group confirmed in correspondence with the authors of this briefing that "Convexum develops and exports the Eclipse anti-drone system."[136]

Although NSO Group Technologies Ltd. is a limited company incorporated and registered in Israel, "NSO Group" is also an umbrella term used by the company and the media to refer to the various related companies described in this briefing, with employees, operating entities and other financial or holding companies around the world. The NSO Group trademark is owned by NSO Group Technologies Ltd.[137]

6.2 THE FRANCISCO PARTNERS YEARS (2014-2019)

[See Diagram 2 at page 32.]

Just a few years after NSO Group Technologies was established, California-based private equity firm **Francisco Partners** took an interest in the company. Francisco Partners' investment in NSO Group, which was reportedly approved by Israel's Ministry of Defense, was announced in March 2014.[138] It acquired a 70% stake in the company for USD$115 million through its Francisco Partners III LP investment fund.[139]

Several changes to NSO Group's corporate structure were undertaken in the lead-up to the Francisco Partners acquisition. On 2 December 2013, the NSO founders incorporated and registered another company in Israel called **L.E.G.D. Company Ltd.**,[140] the name of which was officially changed on 29 May 2016 to Q Cyber Technologies Ltd. (company number 514971522).[141] L.E.G.D. Company / Q Cyber Technologies Ltd. became the majority shareholder and, beginning on 19 March 2014 (the approximate date of the Francisco Partners acquisition), the active director of NSO Group Technologies Ltd.[142]

---

131. Certificate of Incorporation of a Private Limited Company, Company No. 8521034, UK Companies House, 9 May 2013, https://find-and-update.company-information.service.gov.uk/company/08521034/filing-history

132. PFOS Technologies Ltd., *Financial Statements for the Year Ended 31 December 2017*, 7 June 2018.

133. M. Orbach, "NSO Buys Counter-Drone Company Convexum", *CTech by Calcalist*, 12 February 2020, www.calcalistech.com/ctech/articles/0,7340,L-3792634,00.html

134. M. Orbach, "NSO Buys Counter-Drone Company Convexum," *CTech by Calcalist,* 12 February 2020, www.calcalistech.com/ctech/articles/0,7340,L-3792634,00.html; Orbis, *Convexum Ltd. Shareholders History*, accessed 10 July 2020.

135. F2, Eddy Shalev, (n.d.), www.f2vc.com/f2-team/eddy-shalev

136. NSO Group Technologies Ltd. Response to Amnesty International, Privacy International, and SOMO letter, 2 May 2021, at Annex 4.

137. TMView, *NSO Group,* (n.d.), www.tmdn.org/tmview/welcome#/tmview/detail/EM500000018063627

138. O. Hirschauge, "Overseas Buyers Snap Up Two More Israeli Cyber Security Firms," *Haaretz*, 19 March 2014, www.haaretz.com/israel-news/business/.premium-2-more-israeli-cyber-security-firms-sold-overseas-1.5336240

139. Bloomberg L.P., *Francisco Partners III LP current portfolio*, retrieved 8 February 2019 from Bloomberg terminal.

140. State of Israel Corporations Authority, *Company Incorporation Certificate of L.E.G.D. Company Ltd.*, 2 December 2013, available as Exhibit 6 to the Complaint, *WhatsApp Inc. v. NSO Group Technologies Limited,* www.courtlistener.com/docket/16395340/1/1/whatsapp-inc-v-nso-group-technologies-limited/

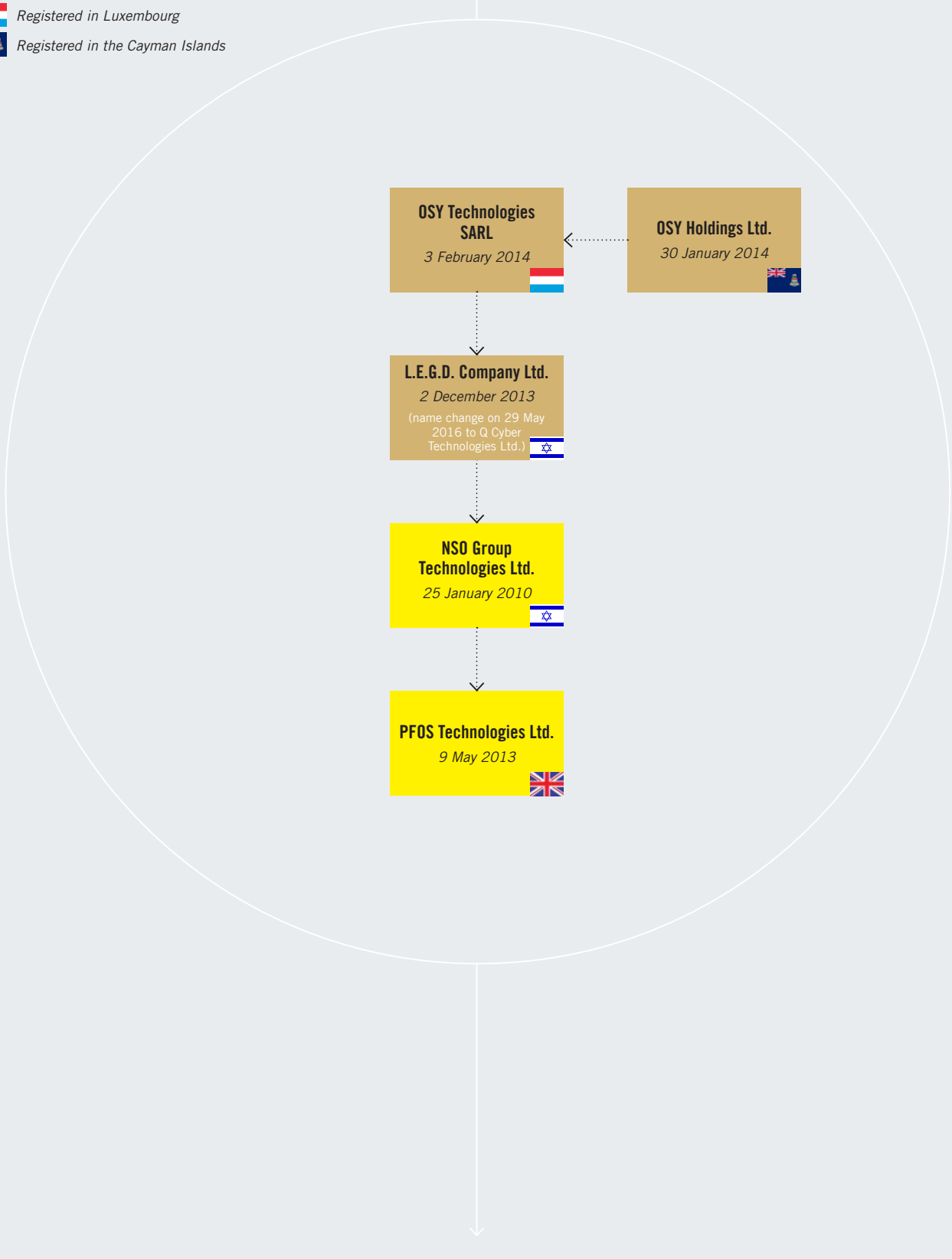
141. State of Israel Corporations Authority, *Company Name Change Certificate of L.E.G.D. Company Ltd.*, 29 May 2016, available as Exhibit 7 to the Complaint, *WhatsApp Inc. v. NSO Group Technologies Limited*, www.courtlistener.com/docket/16395340/1/1/whatsapp-inc-v-nso-group-technologies-limited/

142. State of Israel Corporations Authority, *Private Company Annual Report of NSO Group Technologies Ltd.*, 7 January 2019, available as Exhibit 5 to the Complaint, *WhatsApp Inc. v. NSO Group Technologies Limited*, www.courtlistener.com/docket/16395340/1/1/whatsapp-inc-v-nso-group-technologies-limited/. The annual report notes that NSO Group Technologies Ltd. holds 67,453 (or 36%) of its own allotted ordinary shares. It is unclear which individuals exercise ownership of those shares.

Diagram 2:

Francisco Partners purchase (March 2014) and related preparation

Registered in Israel
Registered in the UK
Registered in Luxembourg
Registered in the Cayman Islands



NSO Group confirmed in correspondence with the authors of this briefing that the "shareholders of NSO Group Technologies Ltd. are Q Cyber Technologies Ltd. and NSO Group Technologies Ltd. itself. Under Israeli law a company may hold its own shares in various instances (such as a buyback). As a result, the full ownership rights of NSO Group Technologies Ltd. are held by Q Cyber Technologies Ltd."[143] It also confirmed that "NSO Group Technologies Ltd. and Q Cyber Technologies Ltd. develop, market and export Pegasus and related analytical products for governmental use. In addition, these entities provide certain sales, marketing services and other administrative support and oversight to their respective affiliates."[144]

OSY Technologies SARL – the first Luxembourg limited liability company to enter the structure – was incorporated on 3 February 2014[145] and became the sole shareholder and active director (beginning March 2014) of L.E.G.D. Company / Q Cyber Technologies Ltd.[146]

The Francisco Partners ownership stake in NSO Group was channelled through OSY Holdings Ltd., a Cayman Islands exempted company registered on 30 January 2014.[147] OSY Holdings Ltd. became the sole shareholder of OSY Technologies SARL when the latter was incorporated on 3 February 2014. While very little documentation is publicly available regarding Cayman Islands companies, during the period of Francisco Partners' ownership of NSO Group, Francisco Partners partners Andrew Kowal[148] and Matthew Spetzler[149] held positions as directors of OSY Holdings Ltd.[150] In correspondence with the authors of this briefing, Francisco Partners confirmed that "[f]rom March 2014 to March 18, 2019 (the 'Sale Date'), Francisco Partners III ('FP III') owned an indirect controlling interest in NSO Group by virtue of its ownership of OSY Holdings Ltd. ('OSY'), which in turn owned a controlling ownership interest in Triangle Holdings, S.A. ('Triangle')." Additionally, Francisco Partners stated that "OSY [Holdings Ltd.] is a Cayman Islands exempted limited partnership that is wholly owned by FP III. OSY is the holding company through which FP III owned its interest in NSO Group prior to its complete exit from the NSO Group business on the Sale Date as described above. OSY has never exported any products or services, and OSY has not engaged in any activities other than holding ownership interests in Triangle, which interests were completely disposed of on the Sale Date. At this time, OSY has no assets or liabilities and is in the process of being dissolved in accordance with Cayman Islands law."[151]

In sum, the structuring of the Francisco Partners acquisition of NSO Group Technologies Ltd. involved the creation of a Cayman Islands company in early 2014, OSY Holdings Ltd., about which few details are publicly disclosed. Francisco Partners utilized OSY Holdings Ltd. to invest as sole shareholder in the new and correspondingly named OSY Technologies SARL, a Luxembourg limited liability company. OSY Technologies SARL became the sole shareholder of an Israeli entity created at the end of 2013, L.E.G.D. Company – later renamed Q Cyber Technologies Ltd. – which at the time of the acquisition became the majority shareholder of NSO Group Technologies Ltd. Francisco Partners' investment fund thus became the ultimate majority owner of NSO Group Technologies Ltd.

---

143. NSO Group Technologies Ltd. Response to Amnesty International, Privacy International, and SOMO letter, 2 May 2021, at Annex 4.

144. NSO Group Technologies Ltd. Response to Amnesty International, Privacy International, and SOMO letter, 2 May 2021, at Annex 4.

145. Registre de Commerce et des Sociétés Luxembourg, Certificate of Registration for Osy Technologies S.à r.l., 3 February 2014.

146. State of Israel Corporations Authority, *Private Company Annual Report of Q Cyber Technologies Ltd.*, 7 January 2019, available as Exhibit 9 to the Complaint, *WhatsApp Inc. v. NSO Group Technologies Limited*, www.courtlistener.com/docket/16395340/1/1/whatsapp-inc-v-nso-group-technologies-limited/

147. Search report: OSY Holdings Limited (Cayman), 3 July 2019; Triangle Holdings, Minutes of Extraordinary General Meeting held on 1 December 2014, www.etat.lu/memorial/2014/C/Html/4019/2014197910.html

148. Registration statement of Ichor Holdings Ltd., www.sec.gov/Archives/edgar/data/1652535/000095012315009869/filename1.htm

149. OSY Technologies SARL, Minutes of Extraordinary General Meeting held on 1 December 2014, www.etat.lu/memorial/2014/C/Html/3988/2014195293.html

150. General Registry, Cayman Islands, *OSY Holdings Limited (Cayman) Director Details*, accessed 28 October 2020.

151. Francisco Partners Response to Amnesty International, Privacy International, and SOMO letter, 27 April 2021, at Annex 3.

[See Diagram 3 at page 35.]

Over the course of 2014, after the Francisco Partners acquisition was completed, a number of other structural changes took place. The Luxembourg-based OSY Technologies SARL acquired the following companies, supplementing Francisco Partners' ownership of L.E.G.D. Company / Q Cyber Technologies Ltd.:[152]

- **IOTA Holdings Ltd.** (registered on 4 November 2014),[153] a Cyprus registered company that is the parent of the following entities: **CS-Circles Solutions Ltd.** (registered on 15 October 2014 in Cyprus),[154] which fully and directly owns **CI-Compass Ltd.** (registered on 23 August 2012 in Cyprus);[155] **Global Hubcom Ltd.** (registered 18 July 2013 in Cyprus);[156] and **MS Magnet Solutions Ltd.** (registered on 10 July 2012 in Cyprus),[157] which fully and directly owns **MI Compass Ltd.** (registered on 24 September 2015 in Cyprus).[158, 159]

  In addition to these Cyprus entities, CS-Circles Solutions Ltd. also owns an entity in Bulgaria, **Circles Bulgaria EOOD**[160] (incorporated in July 2017);[161] and MS Magnet Solutions Ltd owns **Magnet Bulgaria EOOD**[162] (incorporated in April 2014).[163] **These two Bulgarian entities are registered to obtain export licences from the Bulgarian government,[164] suggesting sales of technology or other services from Bulgaria.** Magnet Bulgaria EOOD describes its scope of business activity as (translated):

  > **"Development and distribution of software and hardware, consultancy and product development for private, governmental and non-governmental organizations in the field of computer technology and software and telecommunications, integration of software and telecommunications products, marketing and management, information services, internal and external trade, transport and forwarding activities in the country and abroad, participation in other commercial companies, transactions with intellectual property rights, real estate transactions, letting, and all other activities not prohibited by law."[165]**

  In correspondence with the authors of this briefing, NSO Group noted that "Magnet Bulgaria is currently dormant and inactive. Its registration with the Export Control Authority in Bulgaria expired in 2020 and was not renewed. It has never received licenses for the export of either Vole or Pixcell."[166]

---

152. OSY Technologies SARL, Notes to the annual accounts as at 31 December 2014, §3, Financial Fixed Assets.

153. Registration details for IOTA Holdings Ltd., https://efiling.drcor.mcit.gov.cy/DrcorPublic/SearchResults.aspx?name=%25&number=337445&searchtype=optStartMatch&index=1&lang=EN&tname=%25&sc=1

154. Department of Registrar of Companies and Official Receiver (Cyprus), Certificate of Registration for CS – Circles Solutions Ltd., 15 October 2014.

155. Company information for CI-Compass Ltd., https://opencorporates.com/companies/cy/HE310769

156. Company information for Global Hubcom Ltd., https://opencorporates.com/companies/cy/HE323665

157. Company information for MS Magnet Solutions Ltd., https://opencorporates.com/companies/cy/HE309073

158. Company information for MI Compass Ltd., https://opencorporates.com/companies/cy/HE347278

159. Orbis, *Search report: Iota Holdings Ltd.*

160. Commercial and Non-Profits Organization Register, *Entry for Circles Bulgaria Ltd.*, Republic of Bulgaria Ministry of Justice Registry Agency.

161. Company information for Circles Bulgaria, https://opencorporates.com/companies/bg/175408771

162. Commercial and Non-Profits Organization Register, *Entry for Magnet Bulgaria Ltd.*, Republic of Bulgaria Ministry of Justice Registry Agency.

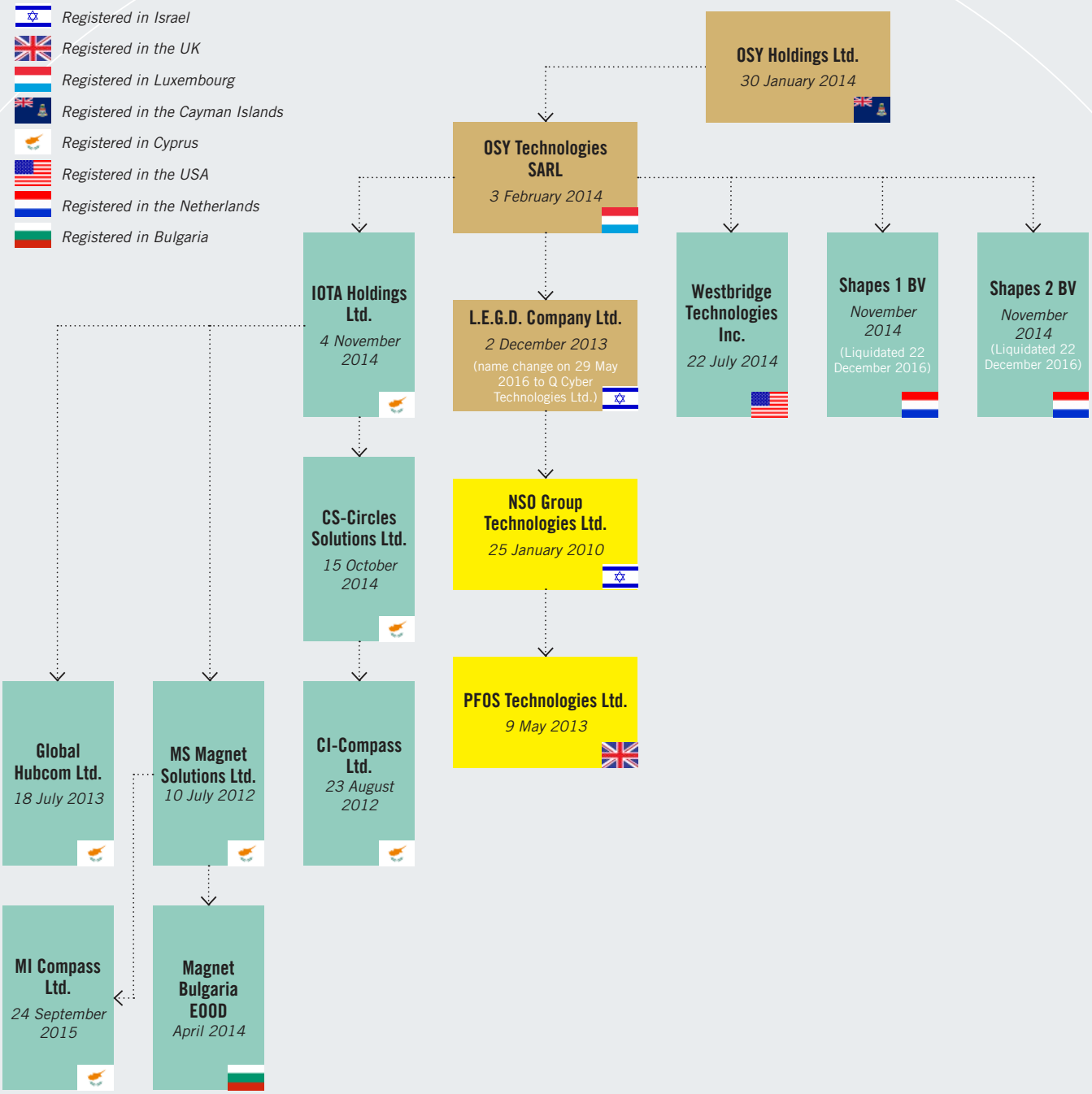
163. Company information for Magnet Bulgaria, https://opencorporates.com/companies/bg/203012611

164. See Republic of Bulgaria Ministry of Economy, "Публичен регистър на лицата, регистрирани за износ и трансфер на изделия и технологии с двойна употреба [Public register of persons registered for export and transfer of dual-use items and technologies]," www.mi.government.bg/files/useruploads/files/exportcontrol/registar_iznos_transfer_22112018.xls, at rows 37 and 61

165. Company information for Magnet Bulgaria, https://opencorporates.com/companies/bg/203012611

166. NSO Group Technologies Ltd. Response to Amnesty International, Privacy International, and SOMO letter, 2 May 2021, at Annex 4.

Diagram 3:
2014 Expansion under Francisco Partners



The Circles enterprise was founded in 2010 by Tal Dilian,[167] Boaz Goldman and Eric Banoun,[168] and is known for developing technology to exploit SS7 vulnerabilities[169] to enable surveillance.[170] As Circles' operating entities are based in Europe, its technology exports would be covered by the EU Dual-Use Export Regulation (EC) 428/2009.[171] The Circles group of companies laid out above was acquired by Francisco Partners for USD$130 million in 2014.[172] NSO Group indicated in correspondence with the authors of this briefing, however, that the Circles-linked entity CT-Circles Technologies Ltd. is not part of the NSO Group group of companies.[173] NSO Group reportedly closed a Cyprus office of Circles in 2020,[174] and it is unclear which Circles-linked corporate entities remain viable.

NSO Group confirmed in correspondence with the authors of this briefing that "[t]he IOTA part of the Group is currently headquartered in Cyprus. Operations are conducted, under contract with the Group's Bulgarian entities, in Bulgaria. . . . The Bulgarian companies provide, on a contract basis, research and development services to their respective Cypriot affiliates and export the network products for governmental use."[175]

- **Westbridge Technologies Inc.**, incorporated in Delaware, USA, on 22 July 2014[176] with Omri Lavie noted as the president or vice president of the company on corporate documentation. Additional branches of this company appear to have been incorporated in Maryland in 2016[177] (which was subsequently dissolved, in June 2019) and Virginia in 2019.[178] According to a LinkedIn page of Terry DiVittorio, former president at Westbridge Technologies Inc., the company:

> **"is the US affiliate of Q Cyber Technologies, a global leader and authority in the world of offensive cyber/cyber-intelligence, target acquisition, and data analysis. Our portfolio of high-end operational and analytical tools, The Q Suite, is shaped by years of focused research, development, and operational experience. The Q Suite is used to combat terrorism and crime as well as preserve national and personal security. Since 2009, our mission has been to equip select intelligence organizations, law enforcement agencies, and military units with strategic, tactical, and analytic capabilities required to ensure the success of their operations."[179]**

---

167. T. Brewster, "A Multimillionaire Surveillance Dealer Steps out of The Shadows... and His $9 Million WhatsApp Hacking Van", *Forbes*, 5 August 2019, www.forbes.com/sites/thomasbrewster/2019/08/05/a-multimillionaire-surveillance-dealer-steps-out-of-the-shadows-and-his-9-million-whatsapp-hacking-van/?sh=45568fe431b7.

168. Prior to founding Circles in 2010, between 2007 and 2010, Eric Banoun was a vice president of sales and business development of the cyber and intelligence business of NICE Systems Ltd. T. Ganon and H. Ravet, "The Dodgy Framework and the Middlemen: How NSO Sold its First Pegasus License," CTech by Calcalist, 24 February 2020, www.calcalistech.com/ctech/articles/0,7340,L-3796112,00.html. His tenure overlapped with the time period during which Francisco Partners' Eran Gorev served as NICE Systems President and CEO, see Bloomberg, Eran Gorev profile, www.bloomberg.com/profile/person/15951007

169. SS7 refers to the "Signaling System 7" network communications protocol. See S. Topuzov, "How vulnerabilities in SS7 protocol expose all mobile networks to attacks", *Secure Group*, 12 June 2017, https://blog.securegroup.com/vulnerabilities-in-ss7-expose-all-networks-to-attacks-why-you-should-be-concerned

170. T. Brewster, "Everything We Know About NSO Group: The Professional Spies Who Hacked iPhones with a Single Text," *Forbes*, 25 August 2016, www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/?sh=30d1cb263997; see also S. Stedman, "The Covert Reach of NSO Group," Forensic News, 29 April 2020, www.forensicnews.net/the-covert-reach-of-nso-group/

171. European Council Regulation (EC) No 428/2009 of 5 May 2009 on setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items, https://eur-lex.europa.eu/eli/reg/2009/428/oj/eng

172. T. Brewster, "Everything We Know About NSO Group: The Professional Spies Who Hacked iPhones with a Single Text," *Forbes*, 25 August 2016, www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/?sh=30d1cb263997

173. NSO Group Technologies Ltd. Response to Amnesty International, Privacy International, and SOMO letter, 2 May 2021, at Annex 4.

174. J. Cox, "NSO Group Closes Cyprus Office of Spy Firm," *Vice*, 21 August 2020, www.vice.com/en/article/ep48kp/nso-group-cyprus-circles-bulgaria-ss7

175. NSO Group Technologies Ltd. Response to Amnesty International, Privacy International, and SOMO letter, 2 May 2021, at Annex 4.

176. State Department of Assessments and Taxation, *Foreign Corporation Qualification: Westbridge Technologies, Inc.,* 30 March 2016.

177. Company information for Westbridge Technologies Inc., https://opencorporates.com/companies/us_md/F17169087

178. Company information for Westbridge Technologies Inc., https://opencorporates.com/companies/us_va/F2128652

179. LinkedIn profile for Terry DiVittorio: www.linkedin.com/in/terry-divittorio-19206a13

Westbridge Technologies Inc. is registered as an active US federal contractor (Commercial and Government Entity [CAGE] code 7FQ39) with Terry DiVittorio named as the point of contact for the US government.[180] Its registration indicated its immediate owner as Francisco Partners GP III Management, LLC (which held its own CAGE code 7A4X2).[181] While the Westbridge Technologies registration information was noted as current and valid until October 2021, Francisco Partners clarified in correspondence with the authors of this briefing that "Francisco Partners GP III is the ultimate general partner of FP III. Neither Francisco Partners GP III nor any other Francisco Partners related entity has ever had any direct ownership interest in Westbridge Technologies, Inc. ('Westbridge'). As described above and for the avoidance of doubt, any indirect ownership interest in Westbridge by Francisco Partners terminated on the Sale Date. Any registration information that shows Francisco Partners GP III as an immediate owner of Westbridge or shows Francisco Partners GP III (or any other Francisco Partners' entity) as a current owner of any interest in any part of NSO Group is false, inaccurate and unauthorized."[182] NSO Group likewise confirmed that the Westbridge Technologies federal contractor registration information was incorrect.[183]

The company's registration in the US and as a federal contractor tends to suggest that Westbridge Technologies Inc. sells technology or other services for the NSO Group in the US. Further, Westbridge has been in contact with the Los Angeles Police Department regarding potential transactions,[184] suggesting it may also work to supply US local law enforcement with services that could potentially include surveillance tools. NSO Group has clarified in correspondence with the authors of this briefing that within the US,

> **"marketing activities are focused on all legitimate governmental users for our Group products in accordance with local laws. Due to various confidentiality constraints we cannot provide specific details, if any, about customers in the US. With respect to the terms referred to in your question 'Q Suite' and 'Phantom,' these are not terms that the Group currently uses in its marketing activities. Moreover, we cannot state with certainty what a former employee meant by their use of the term 'Q Suite.' We assume, probably like you, that this former employee was referring to the various technologies marketed by the Group as they pertain to the market in the United States. Based on the language of the brochure, it would seem that Phantom was a marketing name given to a version of Pegasus at some period of time."[185]**

- **Shapes I BV** and **Shapes 2 BV**, incorporated in November 2014 in the Netherlands, operating in the sectors of "financial holdings" and "engineers and other technical design and advice," respectively.[186] These companies were liquidated just over two years later, on 22 December 2016.[187]

180. Westbridge Technologies Inc. Entity Registration, available at U.S. System for Award Management, www.sam.gov/SAM/pages/public/entitySearch/entitySearchEntityRecord.jsf

181. Westbridge Technologies Inc. Entity Registration.

182. Francisco Partners Response to Amnesty International, Privacy International, and SOMO letter, 27 April 2021, at Annex 3.

183. NSO Group Technologies Ltd. Response to Amnesty International, Privacy International, and SOMO letter, 2 May 2021, at Annex 4.

184. A request for copies of public records made by Mark [Last name redacted] under the California Public Records Act (Request #19-856) on 15 February 2019 for all communication between the Los Angeles Police Department (LAPD) and representatives of WestBridge Technologies Inc, between the dates of 1 January 2017 and 15 February 2019, yielded a January 2018 email exchange from Oren Kaplan of Westbridge to Mark Castillo of the LAPD, "to keep the communication between our organizations and hopefully finish the process we have started a while ago." See https://recordsrequest.lacity.org/requests/19-856

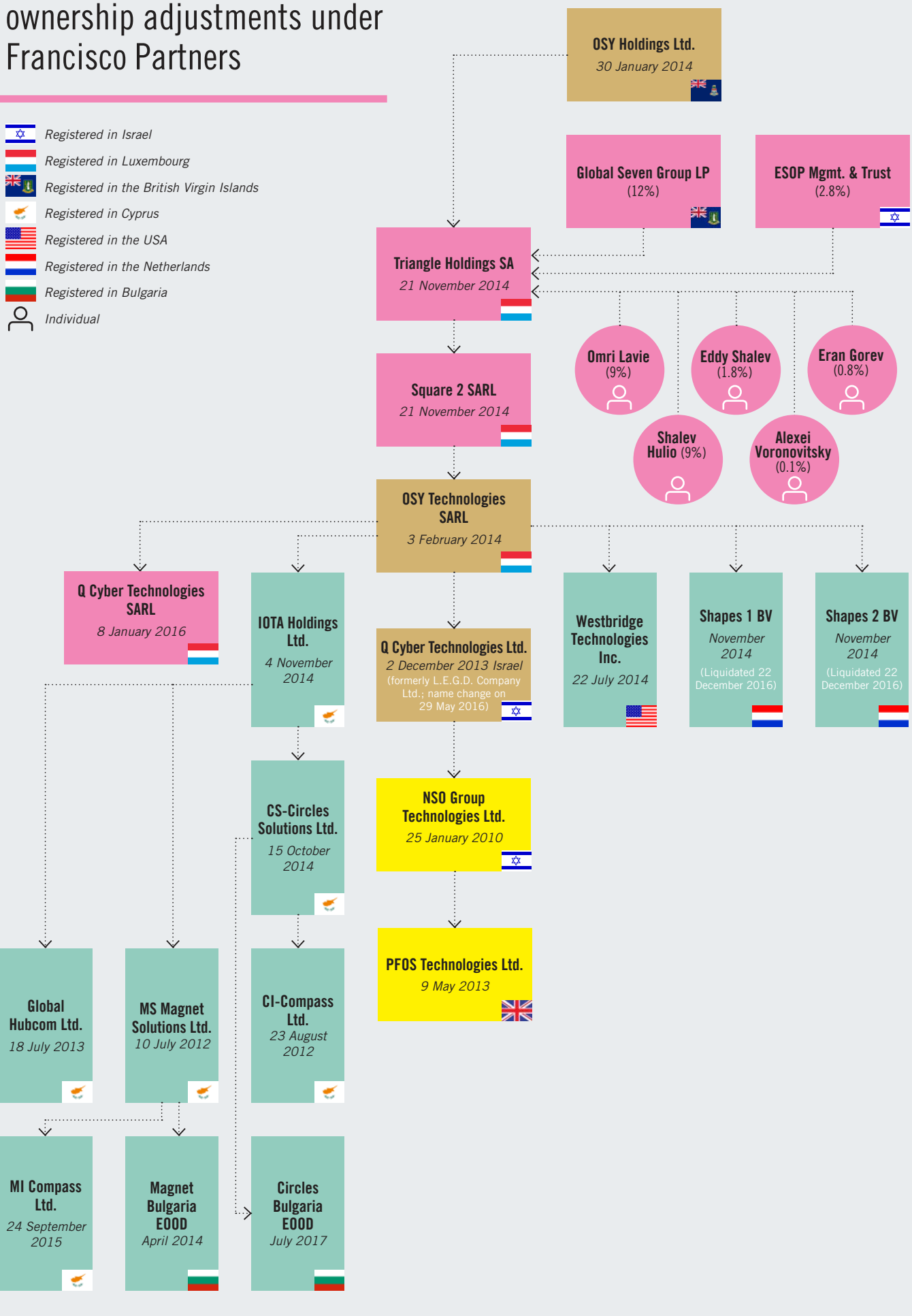
185. NSO Group Technologies Ltd. Response to Amnesty International, Privacy International, and SOMO letter, 2 May 2021, at Annex 4.

186. Company information for Shapes 1 BV, www.oozo.nl/bedrijven/amsterdam/zuidas/zuidas-zuid/1055574/shapes-1-b-v; Company information for Shapes 2 BV, www.oozo.nl/bedrijven/amsterdam/zuidas/zuidas-zuid/1055580/shapes-2-b-v

187. OSY Technologies SARL, Notes to the annual accounts as at 31 December, 2016, §4. Financial Assets.

Diagram 4:

Continued expansion and ownership adjustments under Francisco Partners



Francisco Partners thus actively worked to expand its portfolio of digital surveillance companies through 2014. Indeed, in approximately April to June of that year, representatives of Francisco Partners and NSO Group engaged in merger discussions with Italy-based Hacking Team with an eye to creating a "dominant offensive security beast" in the industry.[188] While that deal did not materialize, the strategy behind it appears to have informed the firm's portfolio expansion.

In late November and early December 2014, two additional levels of holding companies were created in the ownership chain between OSY Holdings Ltd. and OSY Technologies SARL, with NSO-linked individuals this time taking ownership stakes in the holding companies themselves, and thus in the full suite of subsidiary operational companies under OSY Technologies. The new companies followed the geometric-themed naming pattern present elsewhere in the corporate structure: **Square 2 SARL**[189] and **Triangle Holdings SA**[190] were each incorporated in Luxembourg on 21 November 2014. At the time of incorporation, OSY Holdings Limited became the sole shareholder of Triangle Holdings SA, with Francisco Partners director and newly appointed NSO Chair, Eran Gorev its sole director.[191] Triangle Holdings SA, in turn, became the sole shareholder of Square 2 SARL.[192] Square 2 took full ownership of OSY Technologies SARL following share transfers from OSY Holdings Limited.[193]

[See Diagram 4 at page 38.]

OSY Technologies SARL, Square 2 SARL and Triangle Holdings SA each held extraordinary general meetings on 1 December 2014, impacting NSO Group's corporate structure under Francisco Partners' leadership by increasing share capital, as well as adding shareholders to and adjusting board membership of Triangle Holdings SA.

Firstly, reports from the 1 December 2014 meetings show that the share capital of each of the three Luxembourg-based companies was increased. The additional shares at the OSY Technologies and Square 2 levels were subscribed to by their respective sole shareholder / holding company, using shares in the Israel-based NSO Group Technologies Ltd. as payment.[194]

Secondly, at Triangle Holdings SA's 1 December 2014 meeting, its then sole shareholder, OSY Holdings Ltd., resolved to expand ownership of Triangle Holdings SA by allocating certain shares in Triangle Holdings SA to five individuals and two companies as follows:[195]

- British Virgin Islands limited partnership company **Global Seven Group LP (12%)**, which at one point had an ownership interest in CS-Circles Solutions, and may have served as the channel for Circles executives' ownership in Triangle Holdings;[196]

---

188. Email published by WikiLeaks: https://wikileaks.org/hackingteam/emails/emailid/59150. See also: https://wikileaks.org/hackingteam/emails/emailid/54706; https://wikileaks.org/hackingteam/emails/emailid/59610; https://wikileaks.org/hackingteam/emails/emailid/54420; https://wikileaks.org/hackingteam/emails/emailid/56650; https://wikileaks.org/hackingteam/emails/emailid/164292

189. Registre de Commerce et des Sociétés Luxembourg, Certificate of Registration for Square 2, 21 November 2014.

190. Registre de Commerce et des Sociétés Luxembourg, Certificate of Registration for Triangle Holdings, 21 November 2014.

191. Registre de Commerce et des Sociétés Luxembourg, Certificate of Registration for Triangle Holdings, 21 November 2014; see also NSO Group, "NSO Group Acquired by its Management," 14 February 2019, www.nsogroup.com/wp-content/uploads/2019/02/NSO_Group_Acquired_by_its_Management_Feb142019.pdf.

192. Registre de Commerce et des Sociétés Luxembourg, Certificate of Registration for Square 2, 21 November 2014.

193. OSY Technologies SARL, *Transfert de parts Sociales avec Effet au 20 Novembre 2014;* see also Square 2 SARL, Notes to the Annual Accounts as at 31 December 2014, §3. Financial Fixed Assets.

194. OSY Technologies SARL, Minutes of extraordinary general meeting held on 1 December 2014, www.etat.lu/memorial/2014/C/Html/3988/2014195293.html; Square 2 SARL, Minutes of extraordinary general meeting held on 1 December 2014, http://www.etat.lu/memorial/2014/C/Html/3995/2014195459.html, Triangle Holdings SA, Minutes of extraordinary general meeting held on 1 December 2014, www.etat.lu/memorial/2014/C/Html/4019/2014197910.html

195. Triangle Holdings SA, Minutes of extraordinary general meeting held on 1 December 2014, www.etat.lu/memorial/2014/C/Html/4019/2014197910.html

196. S. Stedman, "The Covert Reach of NSO Group," Forensic News, 29 April 2020, https://forensicnews.net/the-covert-reach-of-nso-group/.

- **Omri Lavie,** co-founder of NSO (9%);
- **Shalev Holy (Hulio),** co-founder of NSO (9%);
- Eddy Shalev, an original investor in NSO (1.8%);[197]
- **Alexei Voronovitsky,** a software engineer and former network engineer with the Israel Defense Forces[198] (0.1%);
- **Eran Gorev,** Francisco Partners operating partner and chair of NSO Group (0.8%);
- Israeli trust company **ESOP Management and Trust Services Ltd.** (2.8%), which according to NSO Group "is a company that held shares and options on behalf of employees of the company as part of the Company's Employee Stock Ownership Plan. Applicable tax regulations require establishment of such an entity in order for the Employee Stock Ownership Plan to meet the requirements for tax benefits."[199, 200]

ESOP, Omri Lavie, Shalev Hulio, Eddy Shalev and Alexei Voronovitsky, all used NSO Group Technologies Ltd. shares as contributions in kind to pay for the new Triangle Holdings SA shares.[201] The new shareholders, noted above, had an approximate 35.5% stake in Triangle Holdings SA, while OSY Holdings Ltd., or Francisco Partners, held the remaining 64.5% stake in Triangle Holdings SA.[202]

Thirdly, additional board members were appointed at the Triangle Holdings SA meeting, including Francisco Partners representatives Jonathan Murphy, Andrew Kowal, and Matthew Spetzler; the two NSO Group co-founders Omri Lavie and Shalev Hulio; and Boaz Goldman,[203] who worked with Circles.[204] Shortly thereafter, on 15 December 2014, Eran Gorev was appointed a manager to OSY Technologies SARL.[205] Francisco Partners noted in its correspondence with the authors of this briefing that its "individual professionals serve on the Board of its portfolio companies, where they are responsible for working with each company's management team to set the company's strategic direction. Day-to-day decision-making, including how to respond to press inquiries, falls within the purview of a company's management team and not with the Francisco Partners' individuals who serve on that company's board of directors."[206]

About a year later, on 8 January 2016, a new, Luxembourg-based **Q Cyber Technologies SARL**[207] was incorporated with OSY Technologies SARL as its sole shareholder. At the time of incorporation of Q Cyber Technologies SARL, sole shareholder OSY Technologies SARL appointed Eran Gorev, Kevin

197. Y. Fischer & R. Levy, "The Israelis Behind History's 'Most Sophisticated Tracker Program' that Wormed into Apple", *Haaretz*, 29 August 2016, www.haaretz.com/israel-news/business/.premium-the-most-sophisticated-tracking-program-1.5429923

198. LinkedIn profile for Alexei Voronovitsky: www.linkedin.com/in/alex-v-54397918/, on file with Amnesty International. NSO Group has indicated that "Alexei Voronovitsky is a former consultant that no longer holds shares in any Group company and holds no other positions with the Group." NSO Group Technologies Ltd. Response to Amnesty International, Privacy International, and SOMO letter, 2 May 2021, at Annex 4.

199. NSO Group Technologies Ltd. Response to Amnesty International, Privacy International, and SOMO letter, 2 May 2021, at Annex 4.

200. Triangle Holdings SA, Minutes of extraordinary general meeting held on 1 December 2014, www.etat.lu/memorial/2014/C/Html/4019/2014197910.html

201. Triangle Holdings SA, Minutes of extraordinary general meeting held on 1 December 2014.

202. Triangle Holdings SA, Minutes of extraordinary general meeting held on 1 December 2014.

203. Triangle Holdings SA, Minutes of extraordinary general meeting held on 1 December 2014.

204. T. Brewster, "A Multimillionaire Surveillance Dealer Steps out of The Shadows... and His $9 Million WhatsApp Hacking Van", *Forbes*, 5 August 2019, www.forbes.com/sites/thomasbrewster/2019/08/05/a-multimillionaire-surveillance-dealer-steps-out-of-the-shadows-and-his-9-million-whatsapp-hacking-van/#5eee6b9b31b7; see also T. Brewster, "Everything We Know About NSO Group: The Professional Spies Who Hacked iPhones with a Single Text," *Forbes*, 25 August 2016, www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/#e9f7a0d3997c

205. OSY Technologies SARL, Non-statutory modification, 15 December 2014.

206. Francisco Partners Response to Amnesty International, Privacy International, and SOMO letter, 27 April 2021, at Annex 3.

207. Registre de Commerce et des Sociétés Luxembourg, Certificate of Registration for Q Cyber Technologies, 12 January 2016.

Wilson (former General Counsel at NSO Group),[208] and Yuval Somekh (the "VP Business Operations" of "a Cyber security company," based in Luxembourg)[209] to the company's board of managers. Q Cyber Technologies SARL's articles of association note that the company's corporate objectives include, but also go beyond, holdings and investments: "The Company's purpose shall also be selling and reselling computer software and related physical equipment together with associated consulting, training and the provision of support and other services."[210] The company's annual accounts indicate a net turnover, reflecting "income from sale and distribution of computer equipment and services," in the amounts of USD$24,738,462 in 2016; $82,651,201 in 2017; $169,214,909 in 2018; and $229,839,361 in 2019.[211] The company attributed the significant increase in net turnover between 2017 and 2018 to "higher demand for endpoint solutions".[212] Each of the annual account statements provides that "a breakdown of net turnover by category of activity and into geographical markets is omitted because its nature is such that it would be seriously prejudicial to the Company."[213]

Thus, while the Luxembourg-based Q Cyber Technologies appears to have some active involvement in sales and services, very little information is available on the precise role it plays in NSO Group's overall operations and deployment of NSO Group technology. Notably, the Ministry of Foreign and European Affairs and the Minister of Economy of Luxembourg asserted in February 2019 that the Luxembourg entity linked to NSO Group had never sought an export licence from the Luxembourg authorities.[214] In correspondence with the authors of this briefing, NSO Group provided the following detail regarding Q Cyber Technologies SARL:

> **"Q Cyber Technologies SARL acts as a commercial distributor for the products of the Group companies, as such it signs contracts, issues invoices and receives payments from Group customers. These activities are the basis for reported income. Revenues are recognized in accordance with Generally Accepted Accounting Principles and audited by a leading global auditor. Q Cyber Technologies SARL does not export Group products and has not sought an export license in Luxembourg."[215]**

In summary, in the years immediately following Francisco Partners' investment in NSO Group, the company leadership worked to actively expand surveillance offerings and operational entities, by adding Cyprus- and Bulgaria-based Circles companies to the corporate family; US-based Westbridge Technologies Inc. potentially to facilitate US sales; and the Luxembourg-based Q Cyber Technologies SARL, one corporate objective of which is the provision of services and sales. Around the same time that the Circles entities were integrated, the corporate structure was modified with the addition of two

208. See Novalpina Capital, *Response to Open Letter to Novalpina Capital on 15 April 2019*, www.amnesty.org/download/Documents/DOC1004362019ENGLISH.PDF

209. LinkedIn profile for Yuval Somekh, www.linkedin.com/in/yuvalsomekh/?originalSubdomain=lu

210. Registre de Commerce et des Sociétés Luxembourg, Q Cyber Technologies SARL, Articles of Association, 14 October 2016, at Art. 3.

211. Q Cyber Technologies: Annual Accounts Statement for 2016, 20 June 2017; Annual Accounts Statement for 2017, 18 May 2018; Annual Accounts Statement for 2018, 31 July 2019; Annual Accounts Statement for 2019, 19 November 2020.

212. Q Cyber Technologies, Annual Accounts Statement for 2018, 31 July 2019, at p. 11.

213. Q Cyber Technologies: Annual Accounts Statement for 2016, 20 June 2017; Annual Accounts Statement for 2017, 18 May 2018; Annual Accounts Statement for 2018, 31 July 2019; Annual Accounts Statement for 2019, 19 November 2020.

214. *Réponse écrite de Monsieur Jean Asselborn, Ministre des Affaires étrangères et européennes, Monsieur Etienne Schneider, Ministre de l'Économie*, Chambre des Députés du Grand-Duché de Luxembourg, 19 February 2019, available at www.chd.lu/wps/portal/public/Accueil/TravailALaChambre/Recherche/RoleDesAffaires?action=doQuestpaDetails&id=16839; Dr. Başak Bağlayan, "Mapping the Business and Human Rights Landscape in Luxembourg: National Baseline Study," October 2019, at Annex I pp. 62-63, https://maee.gouvernement.lu/dam-assets/directions/d1/pan-entreprises-et-droits-de-l-homme/Mapping-the-Business-and-Human-Rights-Landscape-in-Luxembourg.pdf

215. NSO Group Technologies Ltd. Response to Amnesty International, Privacy International, and SOMO letter, 2 May 2021, at Annex 4.

levels of Luxembourg-based holding companies above OSY Technologies SARL: Square 2 SARL and its parent company Triangle Holdings SA. These holding companies were used to provide ownership stakes in the full suite of operational companies to key individuals associated with NSO Group and Francisco Partners, including Shalev Hulio, Omri Lavie, Eddy Shalev, Alexei Voronovitsky and Eran Gorev, and presumably with Circles as well (through the opaque Global Seven Group LP). At the start of 2019, Francisco Partners had a 64.5% stake in Triangle Holdings SA through its stake in OSY Holdings Ltd., and NSO Group's founders and financial backers and others had a 35.5% stake in Triangle Holdings SA.

In its correspondence with the authors of this briefing, Francisco Partners indicated that it sold the entirety of its interest in NSO Group on 18 March 2019. It clarified:

> **"On the Sale Date, OSY disposed of 100% of its ownership interest in Triangle, meaning that Francisco Partners had disposed of 100% of its ownership interest in NSO Group and all subsidiaries and businesses that were in any way related to NSO Group. As part of the sale transaction, Eran Gorev also sold 100% of his ownership interest in Triangle. Thus, following the Sale Date, none of Francisco Partners, FP III, OSY, any other legal entity affiliated with Francisco Partners, nor any individual associated with Francisco Partners (including without limitation Eran Gorev) retained any ownership interest or economic interest in, or other rights relating to, NSO Group or any entity that is in any way related to NSO Group. For the avoidance of doubt, it is completely false and inaccurate to assert that any individual or entity associated with Francisco Partners, including without limitation Eran Gorev, has any ongoing ownership interest in, ongoing business relationship with, or ongoing influence or control over, NSO Group or any individual or entity associated with NSO Group. Moreover, since the Sale Date, none of Francisco Partners nor any individual associated with Francisco Partners has any knowledge with respect to the ongoing operations or activities of NSO Group or any of its stakeholders. In addition, since their involvement with NSO Group was purely of a professional nature, each of Eran Gorev, Matt Spetzler and Andrew Kowal resigned from their director roles with NSO Group on the Sale Date."**

Francisco Partners also noted that the ownership interest originally held directly by Eran Gorev in Triangle Holdings SA was "for structuring purposes," and that Gorev "ceased to have any ownership interest in NSO Group and any business associated with NSO Group as of the Sale Date."[216]

6.3 OWNERSHIP CHANGES IN 2019

On 14 February 2019, "[t]he management team and founders of NSO Group... announced the acquisition of the company from global private equity firm Francisco Partners", a management buyout backed by UK-based private equity firm Novalpina Capital.[217] The acquisition announcement described NSO Group as "a cyber-technology company headquartered in Luxembourg" that was "established from the combination of Israeli and European cyber technology companies."[218] With this change in investment and ownership, new companies (using a 'NorthPole' naming convention) were added to the NSO Group corporate structure, linking the structure with Novalpina Capital. The original companies in the structure remained largely intact, although some shareholdings changed. The following section will clarify the corporate structure of the NSO Group of companies following the 2019 ownership changes, as well as the corporate structure of Novalpina Capital.

---

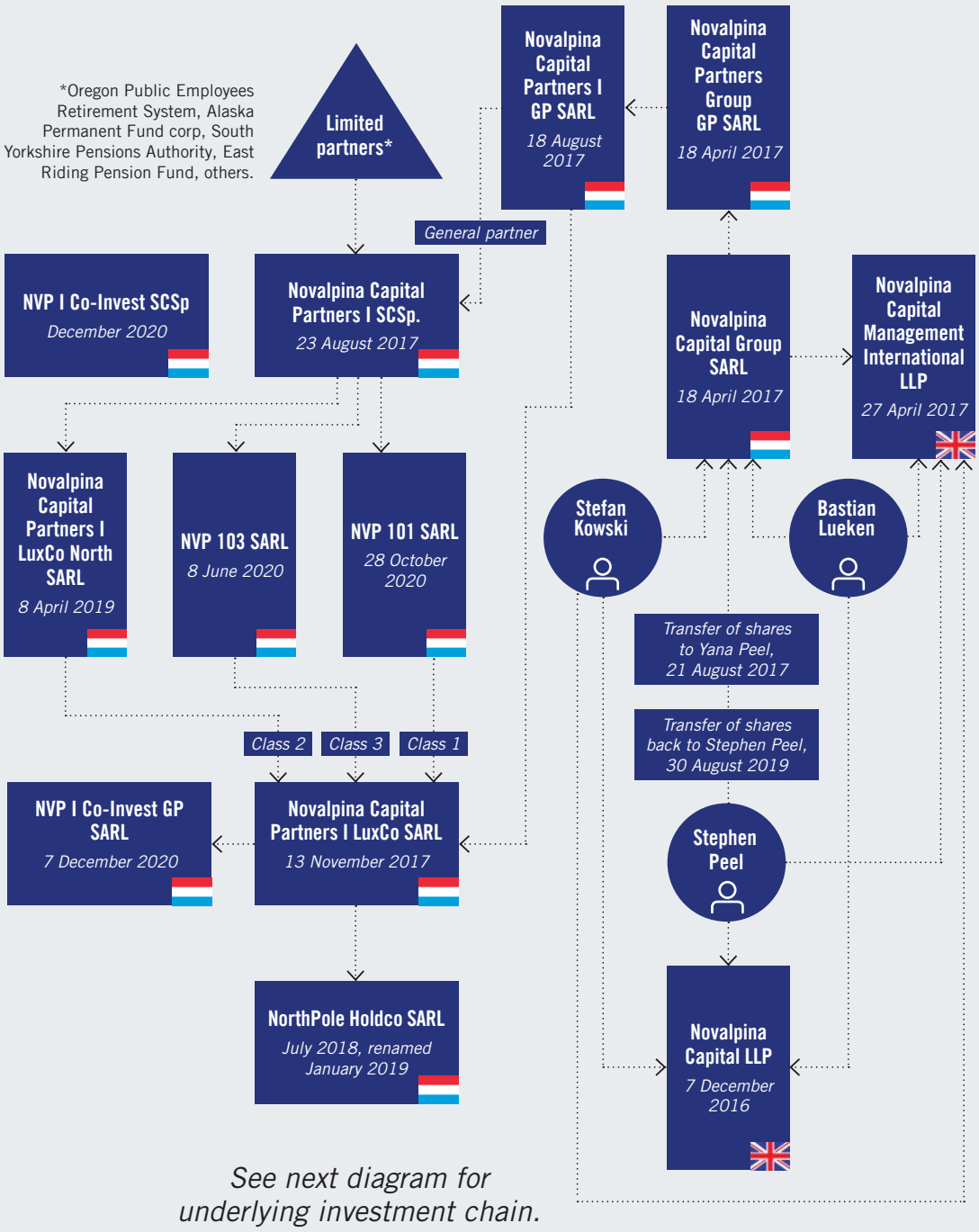
216. Francisco Partners Response to Amnesty International, Privacy International, and SOMO letter, 27 April 2021, at Annex 3.

217. Novalpina Capital, *NSO Group Acquired by its Management*, 14 February 2019, www.novalpina.pe/nso-group-acquired/

218. Novalpina Capital, *NSO Group Acquired by its Management*, 14 February 2019.

Diagram 5:
Novalpina Capital structure

Registered in the UK
Registered in Luxembourg
Individual



See next diagram for underlying investment chain.

NOVALPINA CAPITAL

[See Diagram 5 at page 43.]

Novalpina Capital, the private equity enterprise currently invested in NSO Group, was started in 2017 by partners Stephen Peel, Stefan Kowski and Bastian Lueken.[219] Novalpina's investment focus is on European mid-market companies in sectors "undergoing rapid and disruptive change", where value creation is possible "by capitalizing on both transactional and operational complexity".[220] In a November 2017 presentation to the Oregon Investment Council to secure the Oregon Public Employees Retirement Fund as Novalpina's anchor investor, Novalpina executives described their "rationalist approach" to investing, seeking out investments in which the "operational challenges are such that other people select out of," and being "contrarian... find[ing] deals that other people don't see or don't want to do".[221]

Novalpina Capital's first investment fund is the Luxembourg-based special limited partnership **Novalpina Capital Partners I SCSp** (registered 23 August 2017),[222] which is the private equity fund used to purchase a stake in portfolio companies including NSO Group. Novalpina Capital Partners I SCSp raised money from institutional and other sophisticated investors, which at fund closing had made "total commitments [to the fund] in excess of its target of €1 billion."[223] Novalpina Capital Partners I SCSp's limited partners (investors that have committed capital to the fund) include the **Oregon Public Employees Retirement System** (18%) and the **Alaska Permanent Fund Corp.** (5.1%) in the USA; and **South Yorkshire Pensions Authority** (2.7%) and **East Riding Pension Fund** (1.4%) in the UK.[224]

Novalpina Capital Partners I SCSp's general partner (the entity that manages the investment fund) is **Novalpina Capital Partners I GP SARL**[225] (incorporated 18 August 2017).[226]

Novalpina Capital Partners I GP SARL both manages and itself invests in the fund.[227] The ownership chain in this general partner entity is as follows: Novalpina Capital Partners I GP SARL is wholly owned by **Novalpina Capital Partners I Group GP SARL** (registered 18 April 2017);[228] and Novalpina Capital Partners I Group GP SARL is wholly owned by **Novalpina Capital Group SARL** (incorporated 18 April 2017).[229] At the time of its incorporation, the sole shareholder of Novalpina Capital Group SARL was Stephen Peel.[230]

Ownership adjustments in Novalpina Capital Group SARL took place during the year following its incorporation. On 21 August 2017, Stephen Peel transferred the entirety of his shares to spouse Yana

---

219. Novalpina Capital, *NSO Group Acquired by its Management*, 14 February 2019.

220. TorreyCove Capital Partners memo to Oregon Public Employees Retirement Fund, 25 October 2017, www.oregon.gov/treasury/invested-for-oregon/Documents/oic-meeting-archives/2017/agendas/11.1.2017-OIC-Regular-Meeting-PUBLIC-BOOK.pdf; see also Novalpina Capital, "About Us", (n.d.), www.novalpina.pe/about/

221. Oregon State Treasury, 11/1/2017 Regular Meeting audio file, www.oregon.gov/treasury/invested-for-oregon/Pages/OIC-Meeting-Archive.aspx, at 14:39, 26:20, 29:40

222. Luxembourg Registre de Commerce et des Sociétés, Novalpina Capital Partners I SCSp, Registration, 23 August 2017.

223. Novalpina Capital, "Novalpina Capital Announces the Final Closing of €1 Billion Inaugural Fund," 26 March 2019, https://www.novalpina.pe/final-closing/.

224. Bloomberg L.P., *Novalpina Capital Partners I SCSp Private Equity Fund Holders,* retrieved 19 August 2019 from Bloomberg terminal.

225. Company information for Novalpina Capital Partners, https://opencorporates.com/companies/lu/B217341

226. Novalpina Capital Partners I SCSp, Form D: Notice of Exempt Offering of Securities, U.S. Securities and Exchange Commission, 11 June 2018, www.sec.gov/Archives/edgar/data/1721328/000114420418057650/xslFormDX01/primary_doc.xml

227. "[T]he GP anticipates making a material commitment of €75 million to the partnership." Oregon Investment Council, 1 November 2017, Novalpina Capital Partners I SCSp OPERF Private Equity Portfolio, tab 3, https://www.oregon.gov/treasury/invested-for-oregon/Documents/oic-meeting-archives/2017/agendas/11.1.2017-OIC-Regular-Meeting-PUBLIC-BOOK.pdf

228. Novalpina Capital Partners I GP SARL, Articles of Association, 18 August 2017.

229. Novalpina Capital Group SARL, Articles of Association, 18 April 2017.

230. Novalpina Capital Group SARL, Articles of Association, 18 April 2017.

Peel, such that Yana Peel became sole shareholder of Novalpina Capital Group SARL.[231] At the 29 December 2017 extraordinary general meeting of the company, shareholdings were further modified: 11 new classes of shares were created (class A-K shares); existing shares held by Yana Peel were converted into 1,200,000 Class A shares, which remained exclusive to Yana Peel; share capital was increased by EUR1,200, which was allocated across 12,000 shares in each of class B-K; and the class B-K shares were subscribed equally among Yana Peel, Stefan Kowski and Bastian Lueken (4,000 shares in each class to each shareholder), each of whom paid for their shares through contributions in cash totalling EUR400.[232] On 2 January 2018, Yana Peel's Class A shares were divided equally among Yana Peel, Stefan Kowski and Bastian Lueken, with Yana Peel transferring 400,000 Class A shares to each of the others.[233] On 30 August 2019, Yana Peel transferred the entirety of her shareholdings back to Stephen Peel.[234] Thus, at present, Novalpina Capital Group SARL is owned by Stephen Peel, Stefan Kowski and Bastian Lueken; they are the ultimate owners of the general partner entity Novalpina Capital Partners I GP SARL.

Investments by the Novalpina Capital Partners I SCSp fund in portfolio companies are channelled through the Luxembourg private limited liability company **Novalpina Capital Partners I LuxCo SARL** (incorporated 13 November 2017).[235] Novalpina Capital Partners I LuxCo SARL is utilized as the central holding company for the respective holding companies of the fund's individual portfolio investments. For example, Novalpina's first investment, in a European gambling company, utilized a bidder that was wholly owned by Odyssey Europe Holdco SARL, which was itself wholly owned by Odyssey Europe Topco SARL, of which the sole shareholder was Novalpina Capital Partners I LuxCo SARL.[236] Similarly, in the case of the NSO Group investment, Novalpina utilized the Luxembourg company **NorthPole Holdco SARL** (incorporated July 2018 and renamed in January 2019),[237] which is wholly owned by Novalpina Capital Partners I LuxCo SARL[238] and served as the holding company for the underlying NSO investment chain (see further description below).

At the time of incorporation of Novalpina Capital Partners I LuxCo SARL ("LuxCo"), its sole shareholder was Novalpina Capital Partners I SCSp.[239] At a 29 May 2018 extraordinary general meeting of LuxCo, Novalpina Capital Partners I SCSp created 13 classes of shares within LuxCo: 12 classes of "tracking shares" that would correspond to acquired portfolio companies (see discussion below), held by

231. Novalpina Capital Group SARL, Non-statutory modification, 25 August 2017.

232. Novalpina Capital Group SARL, Extraordinary general meeting, 29 December 2017.

233. Novalpina Capital Group SARL, Non-statutory modification, 12 January 2018.

234. Novalpina Capital Group SARL, Non-statutory modification, 6 November 2019. Earlier that summer, on 18 June 2019, Yana Peel resigned from her position as CEO of the Serpentine Galleries, following public pressure concerning her reported links through Novalpina Capital to NSO Group. J. Swaine et al., "Serpentine Galleries chief resigns", *The Guardian,* 18 June 2019, www.theguardian.com/artanddesign/2019/jun/18/serpentine-galleries-chief-resigns

235. Registre de Commerce et des Sociétés Luxembourg, Articles of Association for Novalpina Capital Partners I LuxCo S.à r.l., 13 November 2017.

236. *Offer Document,* 4 April 2018, https://www.fi.ee/sites/default/files/2018-07/20180402odyssey_offer_document_eng.pdf, at section 4.2 and Annex 4.

237. NorthPole Holdco SARL was formerly a company called Eighteen Scabiosa SARL, registered in Luxembourg in July 2018, which had one shareholder called Alter Domus (Services) Malta Limited. Alter Domus is a company providing "international expertise in the set up and administration of investment structures" to, among others, private equity firms, including "company formation and fund launch." See *Malta Independent,* "Alter Domus starts its 4th year of Malta-based operations", *Malta Independent,* 7 March 2014, https://www.independent.com.mt/articles/2014-03-07/news/alter-domus-starts-its-4th-year-of-malta-based-operations-4176314368/. On 28 November 2018, all 12,000 shares in Eighteen Scabiosa SARL were transferred to Novalpina Capital Partners I LuxCo SARL, and new administrators were appointed. (See Registre de Commerce et des Sociétés Luxembourg, Non-statutory modification, 28 November 2018.) Two months later, on 31 January 2019, an extraordinary general meeting was held and the company name was changed to "NorthPole Holdco SARL" from Eighteen Scabiosa SARL. See Registre de Commerce et des Sociétés Luxembourg, Non-statutory modification, 31 January 2019.

238. Eighteen Scabiosa SARL, Non-statutory modification, 29 November 2018.

239. Novalpina Capital Partners I LuxCo SARL, Articles of Association, 13 November 2017.

Novalpina Capital Partners I SCSp; and one class of priority profit shares.[240] At the same meeting, Novalpina Capital Partners I GP SARL subscribed to the entirety of the priority profit shares of LuxCo through a cash payment of EUR 1.2 million, thus becoming a shareholder in LuxCo as well. At the 19 March 2019 extraordinary general meeting of LuxCo, which took place approximately a month after the announcement of the Novalpina investment in NSO Group, the LuxCo shareholders resolved that LuxCo class 2 tracking shares (a total of 893,750 shares) would track the investment in NorthPole Holdco SARL, which served as the NSO Group-linked holding entity.[241]

In April 2019, a new Luxembourg private limited liability company was added to the structure to hold the LuxCo class 2 tracking shares associated with NSO Group: **Novalpina Capital Partners I LuxCo North SARL** (incorporated 8 April 2019, name changed 8 May 2019)[242] ("LuxCo North"). The sole shareholder of Luxco North was Novalpina Capital Partners I SCSp.[243] At the 8 May 2019 extraordinary general meeting of LuxCo North, Novalpina Capital Partners I SCSp resolved to increase the share capital of LuxCo North by EUR 893,750. Novalpina Capital Partners I SCSp subscribed to the corresponding shares through a contribution in kind of EUR 217,029,827, which consisted of the 893,750 class 2 tracking shares it held in LuxCo valued at EUR 32,564,682, and a receivable in the amount of EUR 184,465,145. LuxCo North thus became the holder of the LuxCo class 2 tracking shares linked to NorthPole Holdco SARL and NSO Group, effectively separating them from the other classes of LuxCo tracking shares held directly by Novalpina Capital Partners I SCSp.[244]

It was not until the latter half of 2020, when Novalpina added new 'NVP' entities to the Novalpina corporate structure, that Novalpina allocated ownership in Novalpina's *other* portfolio companies using an approach similar to that taken with the NSO Group investment, i.e., through distinct holding companies situated above LuxCo. **NVP 103 SARL** was incorporated on 8 June 2020[245] and **NVP 101 SARL** was incorporated on 28 October 2020,[246] with Novalpina Capital Partners I SCSp the sole shareholder of each. Records of the 3 November 2020 extraordinary general meeting of Novalpina Capital Partners I LuxCo SARL reflect the 12 classes of "tracking shares" within the company, which align with Novalpina portfolio acquisitions (Novalpina's three existing acquisitions, and nine classes reserved for future acquisitions). The LuxCo shareholders "resolve[d] to approve that the Investment tracked by the Class 1 Tracking Shares shall be the Company's direct or indirect investment in Odyssey TopCo S.à r.l. and in OEGH Holdings S.à r.l." and "that the Investment tracked by the Class 3 Tracking Shares shall be the Company's direct or indirect investment in Proton JVCo S.à r.l. (to be renamed Hippocrate HoldCo S.à r.l.)."[247] Thus class 1 tracking shares represent Novalpina's first purchase, of the aforementioned gambling company, while class 3 shares appear to represent Novalpina's third purchase,

240. Novalpina Capital Partners I LuxCo SARL, Extraordinary General Meeting, 29 May 2018

241. Novalpina Capital Partners I LuxCo SARL, Extraordinary General Meeting, 19 March 2019, at third resolution.

242. Nineteen Viola S.à r.l., Registration and Articles of Association, 8 April 2019, Luxembourg Registre de Commerce et des Sociétés; Novalpina Capital Partners I LuxCo North SARL, Extraordinary general meeting of 8 May 2019, Luxembourg Registre de Commerce et des Sociétés.

243. Novalpina Capital Partners I LuxCo North SARL, Extraordinary general meeting of 8 May 2019, Luxembourg Registre de Commerce et des Sociétés.

244. Registre de Commerce et des Sociétés Luxembourg, Novalpina Capital Partners I LuxCo North SARL, Extraordinary General Meeting, 8 May 2019.

245. Registre de Commerce et des Sociétés Luxembourg, Twenty Leda SARL, Registration, 8 June 2020 The entirety of the shares in Twenty Leda SARL was transferred to Novalpina Capital Partners I SCSp on 10 August 2020. Registre de Commerce et des Sociétés Luxembourg, Twenty Leda SARL, Modification non statutaire, 13 August 2020. The company name was changed to NVP 103 SARL on 2 November 2020. Registre de Commerce et des Sociétés Luxembourg, Twenty Leda SARL, Extraordinary General Meeting, 2 November 2020.

246. Registre de Commerce et des Sociétés Luxembourg, NVP 101 SARL, Registration, 28 October 2020

247. Registre de Commerce et des Sociétés Luxembourg, Novalpina Capital Partners I LuxCo SARL, Extraordinary General Meeting, 3 November 2020.

the 2020 acquisition of French pharmaceuticals company Laboratoire X.O,[248] the president of which is Hippocrate Pharma.[249] NVP 103 SARL subscribed to the class 3 shares pursuant to resolution at the 3 November 2020 LuxCo extraordinary general meeting. NVP 101 SARL acquired the class 1 shares on 26 November 2020 through a transfer from Novalpina Capital Partners I SCSp.[250] As a result, ownership in each of Novalpina's portfolio companies is ultimately routed through distinct holding companies.

Two other NVP entities were registered at the end of 2020: **NVP I Co-Invest GP SARL** (incorporated 7 December 2020)[251] and **NVP I Co-Invest SCSp**.[252] NVP I Co-Invest GP SARL indicates as its corporate object "(i) the acquisition of participations in one or more corporate partnerships . . . governed by Luxembourg law, including, without limitation, partnerships subject to the law of 23 July 2016 on reserved alternative investment funds . . . in the capacity as general partner . . . of such partnerships and (ii) the management of such partnerships in the capacity as manager."[253] Its sole shareholder is Novalpina Capital Partners I LuxCo SARL.[254] Given the use of "Co-Invest" in the names of these entities and the reference to alternative investment funds in the registration of NVP I Co-Invest GP SARL, it appears NVP I Co-Invest SCSP will be used as a fund for co-investments – "investment opportunities procured by a GP [general partner] which an investor has the discretion to participate in, but are parallel to an existing fund structure"[255] – with NVP I Co-Invest GP SARL as its general partner.

Other relevant Novalpina entities include the two UK-based partnerships that serve as investment advisers[256] to Novalpina Capital Partners I SCSp: **Novalpina Capital LLP** – the private equity firm itself[257] – a limited liability partnership registered in the UK on 7 December 2016, which at the time of registration designated as members Stephen Peel and his company[258] SMP Policy Innovation Ltd.;[259] and **Novalpina Capital Management International LLP,** a limited liability partnership registered in the UK on 27 April 2017, which at the time of registration designated as members Stephen Peel and Novalpina Capital Group SARL.[260] These partnerships have since come to include numerous additional members, while Stefan Kowski, Bastian Lueken, and Stephen Peel are documented as persons with significant control (more than 25% but not more than 50% ownership of voting rights) of each partnership.[261]

---

248. Novalpina Capital, Laboratoire X.O to Embark on New Growth Plan with the Support of Novalpina Capital, 12 November 2020, www.novalpina.pe/laboratoire-x-o-to-embark-on-new-growth-plan-with-the-support-of-novalpina-capital/

249. See Laboratoire X.O profile, "Dirigeants," www.societe.com/dirigeants/laboratoire-x-o-813935863.html

250. Novalpina Capital Partners I LuxCo SARL, Non-statutory modification, 26 November 2020. This document also reflects that Novalpina Capital Partners I SCSp maintains ownership only of Class 4-12 shares, and no longer holds shares in Class 1-3.

251. Registre de Commerce et des Sociétés Luxembourg, NVP I Co-Invest GP SARL, Registration, 7 December 2020.

252. A search for "NVP I Co-Invest" on the Registre de Commerce et des Sociétés Luxembourg search page, available at https://www.lbr.lu, yields reference to NVP I Co-Invest SCSp and lists a 21 December 2020 registration date for the entity.

253. Registre de Commerce et des Sociétés Luxembourg, NVP I Co-Invest GP SARL, Registration, 7 December 2020, at Art. 3.1.

254. Registre de Commerce et des Sociétés Luxembourg, NVP I Co-Invest GP SARL, Registration, 7 December 2020.

255. MJ Hudson, *Private Equity Co-Investments: The Manual,* 2017, https://ilpa.org/wp-content/uploads/2017/02/MJH-Co-Investments-The-Manual.pdf, at p. 5; see also David Greene and Amy Rigdon. "Private equity coinvestment," Latham & Watkins LLP, www.lw.com/thoughtLeadership/private-equity-coinvestment. One noted benefit of the co-investment approach is that "investors have greater control over their capital and have the freedom to decide whether a specific asset is appropriate for their strategy. For instance, an investor can focus on specific sectors or regions. Additional control means that investors can hold some sway on the length of time an investment is held or how the target business is run. Equally important to a co-investor is the ability to sit out an investment opportunity if it does not fit its risk profile." MJ Hudson, supra, at p. 8.

256. Novalpina Capital Partners I SCSp, Notice of Exempt Offering of Securities, 8 November 2017, www.sec.gov/Archives/edgar/data/0001721328/000114420417057216/xslFormDX01/primary_doc.xml

257. LinkedIn page for Novalpina Capital: www.linkedin.com/company/novalpinacapital

258. Certificate of Incorporation of a Private Limited Company, Company No. 10110690, UK Companies House, 7 April 2016.

259. Certificate of Incorporation of a Limited Liability Partnership, Partnership No. OC414979, UK Companies House, 7 Dec 2016.

260. Certificate of Incorporation of a Limited Liability Partnership, Partnership No. OC417109, UK Companies House, 27 April 2017.

261. Novalpina Capital LLP, "People," Partnership No. OC414979, UK Companies House (accessed 14 April 2021); Novalpina Capital Management International LLP, "People," Partnership No. OC417109, UK Companies House (accessed 14 April 2021).

BRINGING TOGETHER THE NOVALPINA AND NSO INVESTOR CAMPS

[See Diagram 6 at page 49.]

The Luxembourg-based company Square 2 SARL, which during Francisco Partners' tenure was wholly owned by Triangle Holdings SA, and which served as the sole shareholder of OSY Technologies SARL, was the company used to bring together the Novalpina and NSO investor camps in 2019. Shortly after the announcement of the ownership change, the board of Triangle Holdings SA met on 18 February 2019 and passed several resolutions in order to prepare for the company to become a part owner in Square 2 SARL, by relinquishing full ownership. These resolutions included: buying back the shares of ESOP Management and Trust Services Ltd. (such that ESOP is no longer a Triangle Holdings shareholder); increasing the company's share capital by issuing new shares; and paying for the new shares through contributions in kind from OSY Holdings Ltd, Global Seven Group LP, Omri Lavie, Shalev Hulio, Eddy Shalev, Eran Gorev and Alexei Voronovitsky.[262]

On 1 April 2019, Triangle Holdings SA held an extraordinary general meeting of its then shareholders where it adopted resolutions to increase the share capital of its wholly owned subsidiary, Square 2 SARL, paid for through contributions in kind from Novalpina Capital's new companies.[263]

On the same day, Square 2 SARL increased its share capital by approximately USD$48 million (from $22 million to $70 million) by issuing new shares valued at $48 million (each share $0.10).[264] Novalpina's NorthPole Holdco SARL agreed to subscribe to the newly issued Square 2 SARL shares valued at $48 million, and pay for them with 100% of the shares it held in Luxembourg private limited liability company **NorthPole Bidco SARL** (incorporated October 2018, renamed in January 2019)[265] valued at $38 million, called the contribution, plus a receivable amounting to $209 million. Square 2 SARL thus became the sole shareholder of NorthPole Bidco SARL. The value of the NorthPole Bidco SARL shares and the receivable together amounted to $247 million. The $199 million in excess of the Square 2 share capital increase was allocated to a Square 2 share premium account.[266]

New managers reflecting Square 2 SARL's new shareholders were appointed to Square 2 SARL's team.[267] Novalpina's appointments included Class A Managers Stefan Kowski, Stephen Peel, Gerhard Schmidt, Mickael Betito, Gunter Maximilian Schmid, and Zamir Dahbash.[268] NSO's appointments included as Class B Managers NSO founders Omri Lavie, Shalev Hulio, and Yuval Somekh.[269]

Additional structural changes modified Square 2 SARL's direct ownership interest in OSY Technologies SARL (which, as noted earlier, is the parent company of a number of NSO operating entities). On 1 April 2019, NorthPole Bidco SARL increased its share capital by USD$22,335,078, from $36,932,246.64 to $59,267,324.64, by issuing new shares valued at $22,335,078 million.

---

262. Registre de Commerce et des Sociétés Luxembourg, Statutory modification, 5 March 2019.

263. Registre de Commerce et des Sociétés Luxembourg, Statutory modification, 1 April 2019.

264. Registre de Commerce et des Sociétés Luxembourg, Statutory modification, 1 April 2019.

265. Similar to the origination of NorthPole Holdco SARL, supra n.237, NorthPole Bidco SARL was originally called Eighteen Lantana SARL and was managed by the Alter Domus (Services) Malta Limited. On 29 November 2018, the Luxembourg-based company Eighteen Scabiosa SARL – which later became NorthPole Holdco SARL – became Eighteen Lantana SARL's sole shareholder after transfer of 12,000 shares. (See Registre de Commerce et des Sociétés Luxembourg, Non-statutory modification, 29 November 2018.) Eighteen Lantana SARL held an extraordinary general meeting in January 2019, where the company's name was changed to NorthPole Bidco SARL. See Registre de Commerce et des Sociétés Luxembourg, Statutory modification, 28 January 2019.

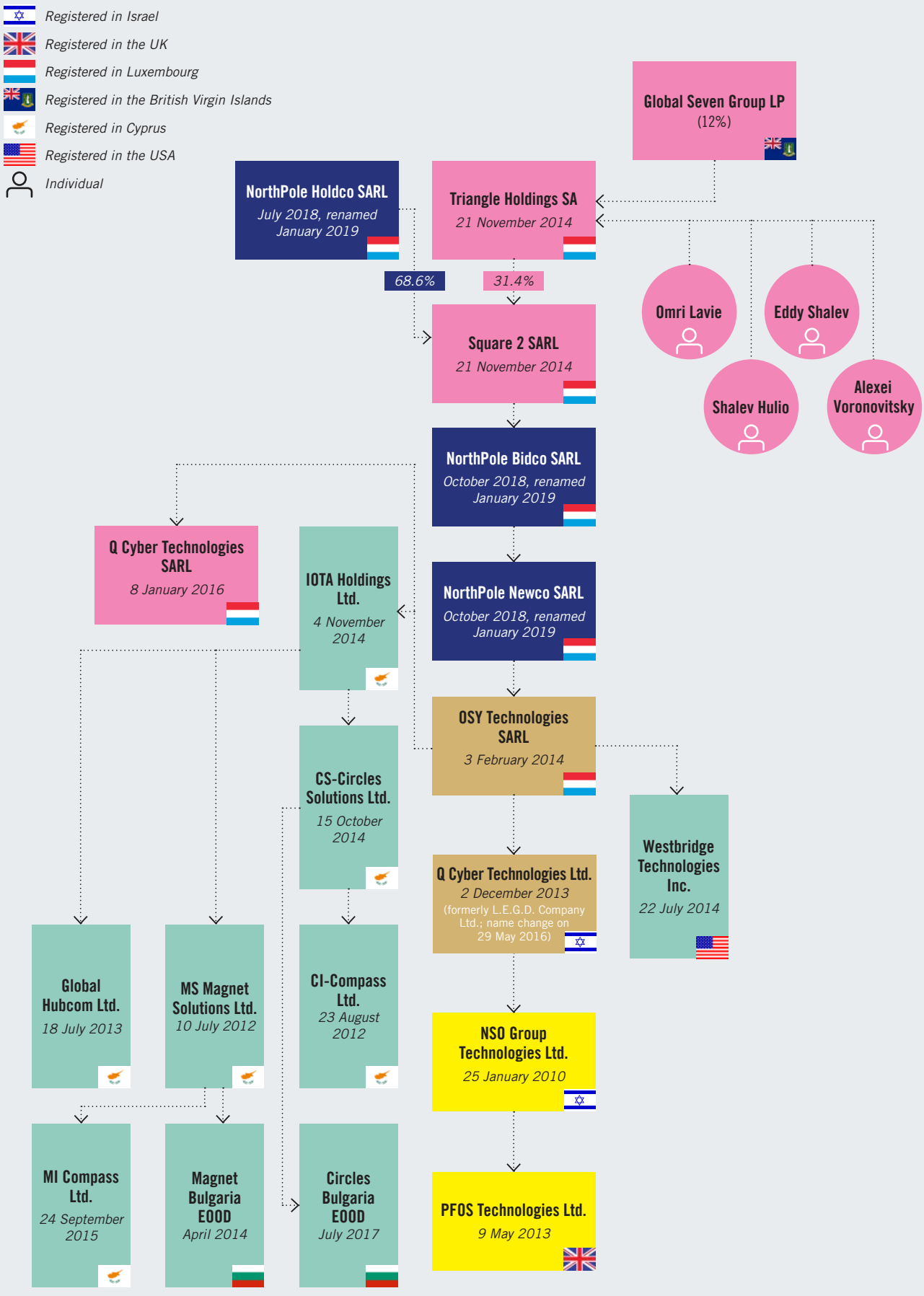
266. Registre de Commerce et des Sociétés Luxembourg, Statutory modification, 1 April 2019.

267. Registre de Commerce et des Sociétés Luxembourg, Statutory modification, 1 April 2019.

268. Novalpina Capital, Response to Open Letter to Novalpina Capital on 15 April 2019, www.novalpina.pe/response-to-open-letter-to-novalpina-capital-on-15-april-2019/

269. LinkedIn profile for Yuval Somekh, https://www.linkedin.com/in/yuvalsomekh/?originalSubdomain=lu

Diagram 6:
Bringing together Novalpina Capital and NSO Group



NorthPole Bidco SARL's sole shareholder, Square 2 SARL, agreed to subscribe to those new shares, by way of a contribution in kind consisting of 100% of the shares it held in OSY Technologies SARL. Thus NorthPole Bidco SARL became the new 100% owner of OSY Technologies SARL. Yuval Somekh was appointed a Class B manager of NorthPole Bidco SARL at the same time.[270] Ownership of OSY Technologies SARL, however, was transferred further that same day to Luxembourg private limited liability company **NorthPole Newco SARL.**[271] NorthPole Newco SARL increased its share capital by approximately USD$22,335,078, by issuing new shares to which its sole shareholder NorthPole Bidco SARL agreed to subscribe, and which NorthPole Bidco SARL paid for by way of a contribution of 100% of those shares it held in OSY Technologies SARL. Again, Yuval Somekh was appointed a Class B manager, this time of NorthPole Newco SARL.[272]

As a result of these April 2019 transactions, the original Square 2 SARL shareholder, Triangle Holdings SA, still owned the original Square 2 SARL shares, or USD$22 million of a total of $70 million (31.4%); the new shareholder, NorthPole Holdco SARL, owned the newly issued Square 2 SARL shares, $48 million of a total of $70 million (68.6%); and Square 2 SARL became the direct and 100% owner of NorthPole Bidco SARL, which owns 100% of NorthPole Newco SARL, which owns 100% of OSY Technologies SARL. OSY Technologies SARL continues to own the operating entities IOTA Holdings Ltd., Q Cyber Technologies SARL, Q Cyber Technologies Ltd., and Westbridge Technologies Inc., as well as their subsidiaries.

Following these changes, executives from both the NSO and Novalpina camps held positions of control within key companies. Triangle Holdings SA's statutes from April 2019 distinguish between two classes of directors and name according to their nominator, as follows: "Any director appointed on the basis of a nomination made by Shalev Hulio and Omri Lavie shall be hereinafter, where applicable, a class B director. Any director appointed on the basis of a nomination made by NorthPole Holdco S.à r.l. via NorthPole Bidco S.à r.l. shall be hereinafter, where applicable, a class A director. The class B directors shall not be authorized to represent the Company, unless the board of directors delegates its powers to such class B directors in accordance with article 12."[273]

Company directors are allocated significant authority under the various entities' articles of association. Article 13b of the Triangle Holdings SA articles lays out a series of "reserved transactions and matters" requiring prior board approval, which the "board of directors shall ensure that the management of any direct or indirect subsidiary shall be bound by."[274] It provides that a majority vote of the directors, *including at least one Class B (NSO-appointed) director*, is required in order to adopt "[s]ignificant changes in the strategic direction of [the] Company and any of its direct or indirect subsidiaries ('Company Group'), in particular, measures and decisions on the strategic and substantive orientation of the Company Group's product offerings, strategic decisions to change and introduce extensive bonus schemes as well as strategic decisions on expansion, limitation or cessation of major distribution channels" (Art. 13.b.1.1.). Notably, a simple majority vote of the directors is required to adopt "Measures and decisions about regulatory affairs, in particular agreements and settlements with export control authorities (e.g. the Israeli Ministry of Defense)" (Art. 13.b.2.7.).

---

270. Registre de Commerce et des Sociétés Luxembourg, Statutory modification, 1 April 2019.

271. Similar to NorthPole Holdco SARL, supra note 237, NorthPole Newco SARL was originally called Eighteen Jasmine SARL, and was managed by Alter Domus (Services) Malta Limited. On 28 January 2019, it was renamed NorthPole Newco SARL. See Registre de Commerce et des Sociétés Luxembourg, Eighteen Jasmine S.à r.l., Extraordinary General Meeting, 28 January 2019.

272. See Registre de Commerce et des Sociétés Luxembourg, NorthPole Newco S.à r.l., Extraordinary General Meeting, 1 April 2019.

273. Triangle Holdings, Articles of Association, 17 April 2019, Article 11.

274. Triangle Holdings, Articles of Association, 17 April 2019, Article 13b.

In keeping with the requirement that all direct and indirect subsidiaries must be bound by these same provisions, Square 2 SARL and NorthPole Bidco SARL likewise make similar distinctions between Class A and Class B directors in their own April 2019 articles of association,[275] and include the same reserved transactions and matters. The April 2019 articles of association of NorthPole Newco SARL[276] and OSY Technologies SARL[277] contain nearly identical provisions as well, though they refer to "managers" instead of "directors." As for board membership, on 1 April 2019, the various corporate entities held extraordinary general meetings at which some individuals associated with Francisco Partners resigned from the companies' boards, and individuals associated with Novalpina Capital joined the relevant boards.

At the Triangle Holdings SA extraordinary general meeting on 1 April 2019, "The Meeting resolve[d] to acknowledge the resignations of Boaz Goldman, Eran Gorev, Andrew Kowal, Jonathan Murphy, Matthew Spetzler as class A directors of the Company and grant provisional discharge (quitus) for the performance of their respective duties from the date of their appointment to the date hereof."[278] At the Square 2 SARL extraordinary general meeting, Triangle Holdings resigned as sole manager of the company, and the following individuals were appointed: as Class A managers, Stefan Kowski, Stephen Peel, Mickael Betito, Gerhard Schmidt,[279] Zamir Dahbash and Günter Maximilian Schmid;[280] and as Class B managers, Omri Lavie, Shalev Hulio and Yuval Somekh.[281]

Similar changes were made to the board of OSY Technologies SARL, with the removal of OSY Holdings Ltd., Eran Gorev and Kevin Wilson, and the appointment of Stefan Kowski, Stephen Peel, Mickael Betito, Gerhard Schmidt, Zamir Dahbash and Gunter Maximillian Schmid (all Class A); and Omri Lavie and Shalev Hulio (Class B).[282]

In correspondence with the authors of this briefing, NSO Group provided the following details regarding board membership:

> **"As a shareholder, Novalpina appoints members to the Group Boards of Directors for Triangle Holdings S.A. and OSY Technologies S.a.r.l. and various committees of those boards, each of which provides strategic direction regarding the activities of the Group. Novalpina is not involved in the day to day, operational activities of the Group, which is the responsibility of Group management. As with any corporation, senior management may consult from time to time with members of the Board on various matters, but Board members are not involved directly in day to day activities."[283]**

NSO Group additionally indicated that the Triangle Holdings SA board of directors (and its committees) regularly discuss "matters related to the strategic direction of the Group and regulatory affairs." Notably, it is the board of Triangle Holdings SA that "adopted various procedures for the implementation of the Group's Human Rights Policy, including the Human Rights Due Diligence Procedure and Product Misuse Investigation Procedure and periodically discusses human rights issues related to the group's activities."[284]

---

275. Square 2, Articles of Association, 1 April 2019; NorthPole Bidco S.à r.l., Articles of Association, 11 April 2019.

276. NorthPole Newco S.à r.l., Articles of Association, 1 April 2019.

277. Osy Technologies S.à r.l, Articles of Association, 1 April 2019.

278. Registre de Commerce et des Sociétés Luxembourg, Triangle Holdings, Extraordinary General Meeting, 1 April 2019, Fifth resolution.

279. Novalpina Capital, *Gerhard Schmidt*, (n.d.), www.novalpina.pe/team/gerhard-schmidt/

280. Novalpina Capital, *Gunter Schmid*, (n.d.), www.novalpina.pe/team/gunter-schmid/

281. Registre de Commerce et des Sociétés Luxembourg, Square 2, Extraordinary General Meeting, 1 April 2019, Fifth resolution.

282. Registre de Commerce et des Sociétés Luxembourg, OSY Technologies S.à r.l., Non-statutory Modification, 12 April 2019.

283. NSO Group Technologies Ltd. Response to Amnesty International, Privacy International, and SOMO letter, 2 May 2021, at Annex 4.

284. NSO Group Technologies Ltd. Response to Amnesty International, Privacy International, and SOMO letter, 2 May 2021, at Annex 4.

On 30 December 2019, one more major structural change took place: the re-routing of the Novalpina Capital investment through Triangle Holdings SA, rather than through Square 2 SARL. At the extraordinary general meeting of Triangle Holdings SA on that date, the Triangle shareholders resolved to increase the share capital of the company by issuing new class A, B and D shares with attached share premium. The nominal value of the newly issued shares totalled USD$38,219.486 and the share premium totalled $247,787,225.514, for a combined value of $247,825,445. NorthPole Holdco SARL fully subscribed to these new shares "by way of a contribution in kind consisting of 484,808,020... shares, with a nominal value of USD 0.1... each, representing 68.46% of the capital of Square 2... and having a fair market value of USD247,825,445."[285] **Thus NorthPole Holdco contributed all of its shares in Square 2 to Triangle Holdings in exchange for an ownership stake in Triangle Holdings, rendering Square 2 a wholly-owned subsidiary of Triangle Holdings, and Triangle Holdings the point of nexus between Novalpina and NSO.** The NorthPole Holdco (i.e., Novalpina) stake in Triangle Holdings amounted to approximately 59.8% of the Class A shares, 21.6% of the Class B shares, and 31.1% of the Class D shares.[286] The Triangle shareholders also appointed Novalpina executives to the company's board of directors, namely, Mickaël Betito, Stefan Kowski, Stephen Peel, Maximilian Schmid Günter and Gerhard Schmidt, as Class A directors, while Shalev Holy [Hulio] and Omri Lavie were reclassified as Class B directors.[287] Additionally, on 27 April 2020, Triangle Holdings SA appointed Asher Levy as a Class A director.[288] Levy was named NSO executive chairman in early April 2020.[289]

At the time of writing, the precise stake of NorthPole Holdco in Triangle Holdings is unclear. While pursuant to the Luxembourg Accounting Law, the notes to the annual accounts of the other Luxembourg-based holding companies associated with NSO Group provide a list of undertakings in which the companies hold at least 20% share capital or in which they are a general partner, NorthPole Holdco does not list such holdings, which would presumably have reflected its stake in Square 2 or Triangle Holdings. It instead notes: "In accordance with Article 67 (1) b) *[of the Luxembourg Accounting Law]*, the information prescribed by Article 65(1)2° relating to all undertakings in which the Company holds at least 20% of the share capital has been omitted, as its nature is such that it would be seriously prejudicial to this/these undertaking(s)."[290] Since December 2019 there have been two additional increases to Triangle Holdings' Class B shares, in March and August of 2020, though it is unclear how those shares were subscribed.[291]

---

285. See Triangle Holdings SA, Minutes of extraordinary general meeting – Capital Increase – Statute Modification, 30 December 2019, Luxembourg Registre de Commerce et des Sociétés.

286. At the 30 December 2019 extraordinary general meeting of Triangle Holdings SA, the share premium was allocated among Class A, B, and D shares as follows: USD$20,021,898.492 attached to new ordinary A shares; USD$13,148,063.937 attached to new ordinary B shares; and USD$214,617,263.085 attached to new ordinary D shares. See Triangle Holdings SA, Minutes of extraordinary general meeting – Capital Increase – Statute Modification, 30 December 2019, Luxembourg Registre de Commerce et des Sociétés, at First Resolution. Additionally, pursuant to the Triangle Holdings SA articles of association, shares of each class A-D are valued at USD$0.001 each, while shareholders of each respective class are entitled to the following rights:
- Class A: voting right and right to dividend;
- Class B: no voting right, but "(i) a preferential cumulative right to dividend equal to 0,001% of the nominal value of an Ordinary B Share, (ii) a further right to dividend in accordance with article 19 and (iii) in case of liquidation of the Company, a preferential right to repayment of the nominal value of such shares together with any premium attached thereto as well as any additional right in accordance with article 23;"
- Class C: no voting right, but "(i) a preferential cumulative right to dividend equal to 0,001% of the nominal value of an Ordinary C Share, and (ii) in case of liquidation of the Company, a preferential right to repayment of the nominal value of such shares together with any premium attached thereto;"
- Class D: voting right and right to dividend.

See Triangle Holdings SA, Consolidated Articles of Association, 20 January 2021, Luxembourg Registre de Commerce et des Sociétés, at Art. 6.

287. Triangle Holdings SA, Minutes of extraordinary general meeting – Capital Increase – Statute Modification, 30 December 2019, Luxembourg Registre de Commerce et des Sociétés.

288. Triangle Holdings SA, *Nomination, renouvellement, fin de mandat des mandataires, des personnes chargées du contrôle des comptes et/ou du dépositaire*, 24 July 2020, Luxembourg Registre de Commerce et des Sociétés.

289. A. Ziv, "Israeli Spyware Company NSO Names Tech Executive as Chairman", *Haaretz*, 7 April 2020, www.haaretz.com/israel-news/business/.premium-israeli-spyware-company-nso-names-tech-executive-as-chairman-1.8748886

290. Registre de Commerce et des Sociétés Luxembourg, NorthPole Holdco SARL, Notes to the annual accounts as at December 31, 2019, 29 October 2020, at p. 9.

291. Triangle Holdings SA, Share capital increase, 5 March 2020, Luxembourg Registre de Commerce et des Sociétés; Triangle Holdings SA, Share capital increase, 7 August 2020, Luxembourg Registre de Commerce et des Sociétés.

Finally, while it is unclear from corporate documentation how the following changes were effectuated, NSO Group asserted in correspondence with the authors of this briefing that: Kevin Wilson, though a former employee, is a current shareholder in Triangle Holdings; former consultant Alexei Voronovitsky "no longer holds shares in any Group company and holds no other positions with the Group;" and "[t]he Group has no companies located in Cayman Islands or the British Virgin Islands. OSY Holdings Ltd. and Global Seven Group LP have no shares or other interest in Triangle Holdings."[292]

[See Diagram 7 at page 58.]

OTHER RECENT DEVELOPMENTS

Additional Q Cyber Technologies Ltd. subsidiaries: Since 2019, Israel-based Q Cyber Technologies Ltd. has been the sole shareholder of two other Israel-based companies including **NGTP Ltd.** (incorporated 20 June 2019, number 516043551)[293] and **S. Sesame Technology Ltd.** (incorporated 5 September 2019, number 516080850).[294, 295] In correspondence with the authors of this briefing, NSO Group noted that "NGTP and Sesame are currently inactive. They were created for potential future plans of the company that have not currently materialized."[296]

Activity on behalf of Q Cyber Technologies Ltd. in the US: In December 2019, not long after the suit was filed against NSO Group by WhatsApp on 29 October 2019,[297] Israel-based Q Cyber Technologies Ltd. hired US public strategy firm Mercury Public Affairs, LLC as a consultant on "government relations and crisis management issues" in connection with the lawsuit and "potential future litigation or regulatory actions involving similar issues."[298] Pursuant to the requirements of the US Foreign Agents Registration Act (FARA), Mercury must disclose the activities it undertakes on behalf of foreign principals.[299] Mercury's FARA filings identify Q Cyber Technologies Ltd. as a foreign principal "[c]ontrolled by a foreign government, foreign political party, or other foreign principal" because "[s]ome of foreign principal's technology offerings are anticipated to be marketed to government clients, and the Ministry of Defense of Israel may deny such sales."[300] Later FARA filings indicate that Mercury engages in "[s]trategic consulting, lobbying, public affairs, and government relations, including outreach to US officials" on behalf of Q Cyber Technologies Ltd.[301]

Changes to NSO Group's advisory committees: As ownership in NSO Group has changed hands, so has the brain trust advising NSO Group. According to Francisco Partners, during the time of its ownership interest in NSO, the company "implement[ed] a best-in-class business ethics framework and [brought] in independent experts to ensure the company was operating in accordance with the

292. NSO Group Technologies Ltd. Response to Amnesty International, Privacy International, and SOMO letter, 2 May 2021, at Annex 4.

293. Entry for NGTP Ltd., Israeli Corporations Authority, https://ica.justice.gov.il (accessed 14 April 2021).

294. Entry for S. Sesame Technology Ltd., Israeli Corporations Authority, https://ica.justice.gov.il (accessed 14 April 2021).

295. Israel Business Registry, November 2019.

296. NSO Group Technologies Ltd. Response to Amnesty International, Privacy International, and SOMO letter, 2 May 2021, at Annex 4.

297. See Court Listener, Docket Entries: *WhatsApp Inc. v. NSO Group Technologies Limited* (4:19-cv-07123), https://www.courtlistener.com/docket/16395340/whatsapp-inc-v-nso-group-technologies-limited/

298. See Mercury Public Affairs, LLC, Exhibit A to Registration Statement Pursuant to the Foreign Agents Registration Act of 1938, Schedule 1, https://efile.fara.gov/docs/6170-Exhibit-AB-20191225-73.pdf.

299. Department of Justice, *Frequently Asked Questions,* 3 December 2020, www.justice.gov/nsd-fara/frequently-asked-questions

300. See Mercury Public Affairs, LLC, Exhibit A to Registration Statement Pursuant to the Foreign Agents Registration Act of 1938, https://efile.fara.gov/docs/6170-Exhibit-AB-20191225-73.pdf

301. See Mercury Public Affairs, LLC, Short Form Registration Statement Pursuant to the Foreign Agents Registration Act of 1938, https://efile.fara.gov/docs/6170-Short-Form-20200108-582.pdf

highest ethical standards"[302] through a "Business Ethics Committee" (BEC). The BEC provided a final layer of review, after export licences were obtained from government authorities, to deny or approve a sale or discontinue service of surveillance technology to government clients – effectively giving the committee enormous influence over exports that could seriously undermine human rights.[303] Francisco Partners confirmed in correspondence with the authors of this briefing that the BEC "reviewed all potential sales and addressed alleged cases of misuse. Under Francisco Partners' ownership of NSO Group, the BEC blocked tens of millions of dollars in sales that would have otherwise been permitted based on applicable legal requirements."[304]

According to Novalpina Capital, "the BEC [was] a key committee of the NSO Board and comprise[d] 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."[305] While the company did not disclose the members' identities, media reporting indicates the committee included Daniel Reisner, a partner at the Israeli law firm Herzog Fox & Neeman, as a member.[306] Daniel Reisner has continued his work with NSO Group by advising Novalpina Capital regarding limitations under Israeli export law on sharing of information related to NSO exports.[307]

Following acquisition by Novalpina Capital and the related governance changes, the BEC was replaced by a Governance, Risk and Compliance Committee (GRCC).[308] This committee has similar powers to "reject sales or request investigations into potential misuse".[309] NSO Group confirmed in January 2021 that its "Governance, Risk and Compliance Committee is in operation... The GRC is NSO's ultimate committee for reviewing human rights and compliance issues and takes every possible step to ensure that our technology is sold only to customers who will use it as intended: to prevent and investigate terror and serious crime."[310]

In correspondence with the authors of this briefing, NSO Group detailed that the GRCC is a board-level committee appointed by the OSY Technologies SARL board of directors, which oversees full investigations into allegations of misuse deemed credible.[311] The GRCC "meets on a monthly basis and its discussions relate to the human rights issues of the group's activities," regarding which it seeks out advice from "a group of internationally recognized advisers that have significant experience in the fields relevant to our activities." The following individuals sit on the GRCC: an independent director; the

302. NSO Group, "NSO Group Acquired by its Management," 14 February 2019, www.nsogroup.com/wp-content/uploads/2019/02/NSO_Group_Acquired_by_its_Management_Feb142019.pdf.

303. "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 also must approve the renewal of maintenance contracts." Novalpina Capital, *Response to Open Letter to Novalpina Capital on 18 February 2019*, www.amnesty.org/download/Documents/DOC10021020 19ENGLISH.PDF

304. Francisco Partners Response to Amnesty International, Privacy International, and SOMO letter, 27 April 2021, at Annex 3.

305. Novalpina Capital, *Response to Open Letter to Novalpina Capital on 18 February 2019.*

306. A. Wenkert, "Israeli Surveillance Company Contests Claims its Technology Played a Role in Khashoggi's Murder," CTech by Calcalist, 14 January 2019, www.calcalistech.com/ctech/articles/0,7340,L-3754228,00.html ("NSO has its own internal ethics apparatus, headed by Daniel Reisner, a partner at Israeli law firm Herzog, Fox & Neeman, and the former head of the international law branch of the Israeli military, according to the report by Yedioth Ahronoth.... Reisner told Yedioth Ahronoth that NSO has ruled out deals valued at nearly $150 million in the past three years when the company assessed there is a chance the client will misuse the technology.")

307. Novalpina Capital, *Response to Open Letter to Novalpina Capital on 15 April 2019*, www.amnesty.org/download/Documents/DOC1004362019ENGLISH.PDF

308. NSO Group, *Governance*, (n.d.), www.nsogroup.com/governance/

309. NSO Group, *Governance*, (n.d.), www.nsogroup.com/governance/

310. See "Answers attributable to an 'NSO Spokesperson'", filed by Mercury Public Affairs, LLC, 7 January 2021, https://efile.fara.gov/docs/6170-Informational-Materials-20210107-802.pdf

311. NSO Group Technologies Ltd. Response to Amnesty International, Privacy International, and SOMO letter, 2 May 2021, at Annex 4.

"Group CEO" (which at time of publication was Shalev Hulio); and "at least two additional directors, one of whom is the Group General Counsel." GRCC members are not provided any "specific or additional compensation" for their work on the committee.[312]

Additional responsibilities of the GRCC include:

> **"approving, monitoring and reviewing the Group's policies regarding governance, risk and compliance, as well as having a veto right on certain of the Group's business opportunities, including the Group's products and services, in accordance with the Human Rights Due Diligence Procedure and overseeing the Group's adherence to our corporate social responsibility principles. The GRCC advises every company in the Group, including, but not limited to IOTA and its subsidiaries."[313]**

In September 2019, Novalpina Capital announced that "it will add three new senior advisors, including Governor Tom Ridge, the first U.S. Secretary of Homeland Security; Gèrard Araud, former French ambassador to the U.S.; and Juliette Kayyem, former Assistant Secretary at the U.S. Department of Homeland Security and a professor at Harvard University's John F. Kennedy School of Government".[314] It is not clear whether these individuals sat on the GRCC or served as the separate group of advisers to the committee. However, NSO Group indicated in January 2021 that these advisers had concluded their work with the company;[315] indeed, Juliette Kayyem resigned from the committee in February 2020 after concerns were raised about the impact of NSO Group technology on journalists.[316]

Potential initial public offering on the Tel Aviv Stock Exchange: As of early 2021, NSO Group is reportedly in discussion with executives at the Tel Aviv Stock Exchange about going public.[317] Shalev Hulio has indicated in media reports that "NSO has two possible paths to a future injection of major funding – an investment from a private investor or an initial public offering," utilizing a special purpose acquisition company; and that if NSO goes public, Hulio will step back from his role as CEO and take up a different position within the company.[318] It is unclear how an initial public offering would affect current shareholdings, how NSO Group could meet the transparency requirements for public trading on the Tel Aviv Stock Exchange, or whether the Israeli Ministry of Defense would approve such a move. Recent modifications to the corporate structure, however, do account for an exit from investment in NSO Group companies (see following text).

New corporate entities and acquisition linked to NorthPole Bidco SARL: On 7 February 2020, Luxembourg private limited liability company **Emerald LIE SARL** was incorporated with NorthPole Bidco SARL as its sole shareholder.[319] NorthPole Bidco SARL subscribed to the entirety of the Emerald shares "by way of a contribution in kind consisting of a receivable of an amount of USD 20,000... it

312. NSO Group Technologies Ltd. Response to Amnesty International, Privacy International, and SOMO letter, 2 May 2021, at Annex 4.

313. NSO Group Technologies Ltd. Response to Amnesty International, Privacy International, and SOMO letter, 2 May 2021, at Annex 4.

314. See: Legal Newswire, "NSO Group Announces New Human Rights Policy and Governance Framework", *Law.com*, 10 September 2019, www.law.com/legalnewswire/news.php?id=1817939

315. See "Answers attributable to an 'NSO Spokesperson'", filed by Mercury Public Affairs, LLC, 7 January 2021, https://efile.fara.gov/docs/6170-Informational-Materials-20210107-802.pdf

316. See: S. Kirchgaessner, "Ex-Obama official exits Israeli spyware firm amid press freedom row", *The Guardian,* 4 February 2020, www.theguardian.com/world/2020/feb/04/ex-obama-official-juliette-kayyem-quits-israeli-spyware-firm-amid-press-freedom-row

317. Reuters, "Israeli cyber firm NSO Group mulls Tel Aviv IPO at $2 billion value – reports", *Reuters*, 6 January 2021, https://www.reuters.com/article/israel-cyber-nso-ipo-int-idUSKBN29B0WU

318. Amitai Ziv, "Controversial Israeli Spyware Firm NSO Eyes Public Listing, CEO May Step Down," *Haaretz*, 23 March 2021, https://archive.li/GxYZe#selection-431.0-431.77.

319. Registre de Commerce et des Sociétés Luxembourg, Emerald LIE, Registration, 7 February 2020.

holds against Osy Technologies S.à r.l."[320] That same day, Emerald LIE became the sole shareholder of newly incorporated Luxembourg private limited liability company **Diamond LIE SARL**, subscribing to the entirety of the share capital with the USD$20,000 OSY Technologies receivable.[321] Gaëtan Dumont was appointed Type A manager, and Yuval Somekh Type B manager, of each company.[322] In correspondence with the authors of this briefing, NSO Group noted that "Emerald and Diamond are companies created for the sake of granting stock options to management, directors and employees under stock option plans."[323]

On 5 February 2020, NorthPole Bidco SARL acquired **Goatilev Ltd.**, "a shelf company incorporated under the laws of the State of Israel, which acquired two companies incorporated under the laws of the State of Israel in February 2020 and March 2020."[324] Goatilev is reported to have purchased Wayout, a surveillance company that "specialises in compromising routers for cyber-intelligence operations by police and intelligence agencies" and "focuses particularly on the interception of Internet of Things (IoT) data," in 2020.[325] NSO Group confirmed in correspondence with the authors of this briefing that Wayout is an NSO Group company that "develops cyber security products for the IoT world for governmental use."[326]

At an extraordinary general meeting of Emerald LIE on 30 November 2020, NorthPole Bidco SARL contributed the entirety of the shares it held in Goatilev and NorthPole Newco to Emerald LIE "for an aggregate amount of USD$326,800,326.27 in consideration for the issuance by Emerald of 350,000,000 new preferred B shares, with a nominal value of USD$0.001 to [NorthPole Bidco] and a share premium attached thereto of USD$326,450,326.27."[327] At the extraordinary general meeting of Diamond LIE that same day, Emerald LIE replicated the aforementioned transaction in contributing those same Goatilev and NorthPole Newco shares to Diamond LIE.[328] As a result, Emerald LIE and Diamond LIE were inserted directly into the chain of NSO Group Technologies holding companies, between NorthPole Bidco SARL and NorthPole Newco SARL; and the Goatilev companies acquired by NorthPole Bidco SARL are now held by Diamond LIE alongside NorthPole Newco SARL.

Notably, also at the time of the 30 November 2020 extraordinary general meetings of Emerald LIE and Diamond LIE, provisions concerning exit from investment in NSO Group corporate entities were added to the articles of association of the two companies. For example, the revised articles define "exit" as

> **"(i) an IPO with respect to all or substantially all shares of the relevant entity, (ii) a Disposal of all or substantially all assets of, or shares in, Triangle and/or the Company [Emerald LIE SARL] and/or Diamond LIE SARL and/or NorthPole Newco S.à r.l. or the shares**

320. Registre de Commerce et des Sociétés Luxembourg, Emerald LIE, Registration, 7 February 2020.

321. Registre de Commerce et des Sociétés Luxembourg, Diamond LIE, Registration, 7 February 2020.

322. Registre de Commerce et des Sociétés Luxembourg, Emerald LIE, Registration, 7 February 2020; Registre de Commerce et des Sociétés Luxembourg, Diamond LIE, Registration, 7 February 2020.

323. NSO Group Technologies Ltd. Response to Amnesty International, Privacy International, and SOMO letter, 2 May 2021, at Annex 4.

324. Registre de Commerce et des Sociétés Luxembourg, NorthPole Bidco SARL, Notes to the annual accounts from October 5, 2018 to December 31, 2019, 9 March 2021, at p. 19.

325. "Discreet startup Wayout gathers intelligence from IOT devices," Intelligence Online, 4 March 2021, www.intelligenceonline.com/surveillance--interception/2021/03/04/discreet-startup-wayout-gathers-intelligence-from-iot-devices%2C109647804-ar1

326. NSO Group Technologies Ltd. Response to Amnesty International, Privacy International, and SOMO letter, 2 May 2021, at Annex 4.

327. Registre de Commerce et des Sociétés Luxembourg, NorthPole Bidco SARL, Notes to the annual accounts from October 5, 2018 to December 31, 2019, 9 March 2021, at p. 19; see also Registre de Commerce et des Sociétés Luxembourg, Emerald LIE, Extraordinary General Meeting, 30 November 2020, at fourth resolution.

328. Registre de Commerce et des Sociétés Luxembourg, NorthPole Newco SARL, Notes to the annual accounts from December 5, 2018 to December 31, 2019, 9 March 2021, at p. 17; see also Registre de Commerce et des Sociétés Luxembourg, Diamond LIE, Extraordinary General Meeting, 30 November 2020, at fourth resolution.

in all or substantially all of their subsidiaries, or (iii) the Disposal of all or substantially all of the shares in the Controlling Parent or any other transaction, which is qualified as an Exit by the Controlling Parent (or any Affiliate thereof) and notified to the Participant and has substantially the same economic effect as the transactions mentioned under (i) and (ii), except for transactions with any of Investor's Affiliates (as purchasers) or other related party transactions[.]"[329]

As used in this definition, "IPO" means "an initial public offering of any shares in Triangle, the Company [Emerald LIE SARL], NewCo or any other entity which is holding all or substantially all assets of the Target Group ["Triangle together with all of its direct and indirect subsidiaries"]."[330] "Controlling Parent" means "the majority shareholder of Triangle as of the date when this provision is first included in the articles," namely, NorthPole Holdco SARL.[331]

The articles also provide a distribution waterfall for exit proceeds, which indicates the order in which payments out of the proceeds generated by the sale are to be made to entities and individuals holding stakes in the company. The provision designates that the holders of the preferred B shares are to receive outstanding accrued interest, followed by USD$370 million. (The newly issued preferred B shares in Emerald LIE, together with 20 million existing preferred B shares – for a total of 370 million preferred B shares – are held by NorthPole Bidco.) Remaining exit proceeds up to USD$18.5 million are to be distributed to holders of ordinary A shares. (New ordinary A shares were created at the 30 November 2020 extraordinary general meetings and subscribed to in their entirety by Israeli trust company ESOP Management and Trust Services Ltd., which holds those shares on behalf of "Participant[s]," that is, "key managers of Triangle and of the Company's subsidiaries . . . ."[332])[333] Further parameters are outlined for any additional proceeds.

329. Registre de Commerce et des Sociétés Luxembourg, Emerald LIE, Extraordinary General Meeting, 30 November 2020, at fifth resolution, Art. 33.

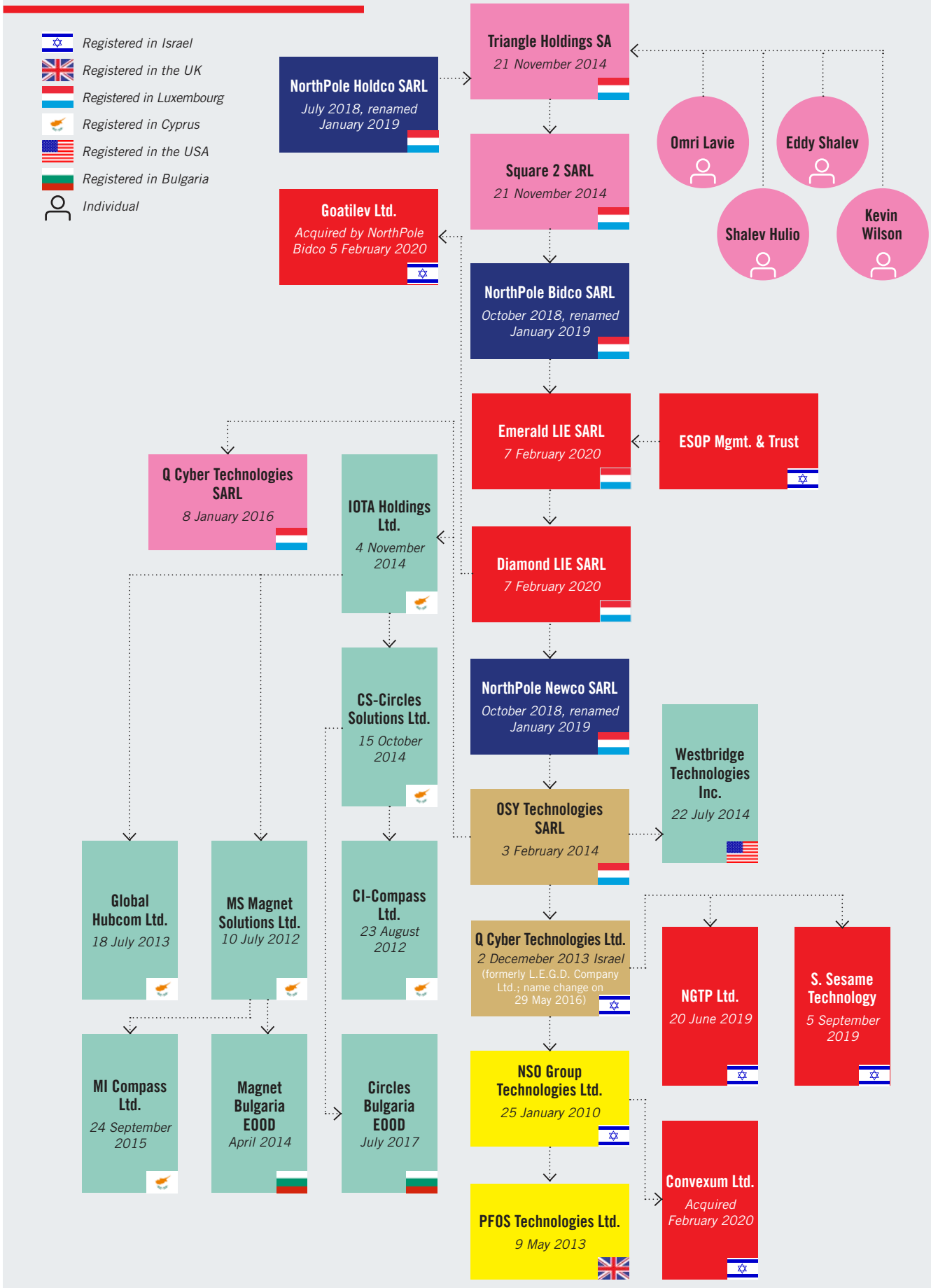
330. Registre de Commerce et des Sociétés Luxembourg, Emerald LIE, Extraordinary General Meeting, 30 November 2020, at fifth resolution, Art. 33.

331. Registre de Commerce et des Sociétés Luxembourg, Emerald LIE, Extraordinary General Meeting, 30 November 2020, at fifth resolution, Art. 33.

332. Registre de Commerce et des Sociétés Luxembourg, Emerald LIE, Extraordinary General Meeting, 30 November 2020, at fifth resolution, Art. 33.

333. Registre de Commerce et des Sociétés Luxembourg, Emerald LIE, Extraordinary General Meeting, 30 November 2020, at fifth resolution, Art. 27.3.

Diagram 7:
Further refinements under Novalpina Capital



7. APPLYING THE RESPONSIBILITY TO RESPECT HUMAN RIGHTS ACROSS THE NSO CORPORATE FRAMEWORK

The deployment of surveillance tools provided by NSO Group to government entities around the world, and subsequent documentation of deployment against human rights defenders and civil society at large, exemplifies how readily surveillance technology can be used to undermine human rights, and the willingness of the private sector and governments to engage in and/or tolerate such abuses in pursuit of profits and geopolitical advantage. Legal and regulatory frameworks, such as export licensing frameworks or domestic legal safeguards, have not kept pace with the growth of the surveillance industry. This, coupled with the lack of transparency in the industry, creates risks that are not yet fully appreciated or accounted for by governments or the private sector. Despite clear evidence of misuse, an absence of human rights safeguards, and increasing demands for accountability, surveillance companies and a wide range of investors and financial backers have continued to capitalize on the digital surveillance trade.

As noted in Section 4 above, the UNGPs apply to all business enterprises, including digital surveillance companies, as well as the private equity firms, limited partners and other corporate entities which have invested funds or otherwise participate in the digital surveillance trade. The UNGPs provide the foundation on which participants in the digital surveillance trade can work to fulfil their responsibility to respect human rights, and prevent, mitigate, and remedy adverse human rights impacts. By doing so, these corporate entities will also reduce their own legal and reputational risks.

Additionally, under OECD Guidelines Chapter II (General Policies) article 1022, companies are expected to conduct due diligence to prevent adverse human rights impacts from their activities. Importantly, this responsibility exists even if the company does not itself cause the impact; the company is expected to seek to prevent adverse impacts that are caused by another entity, even if this is a government, if there is a risk that the impact would be directly linked to the company's products or services through a business relationship.[334]

334. Organisation for Economic Co-operation and Development, *Guidelines for multinational enterprises*, www.oecd.org/corporate/mne/

NSO Group and its operating entities have a responsibility to ensure not only that their own activities – such as software development, training, trouble-shooting or other forms of client support – do not cause or contribute to human rights abuses, but also that they take steps to prevent and mitigate adverse human rights impacts otherwise linked to their operations through business relationships, including through client deployment of their technology.[335] They also have the responsibility to engage in remediation in case of harm. Hence, NSO Group must identify and assess the risks of their products' end-user violating human rights. This includes an assessment of a number of factors, such as the end-user's intention for the use of the product and services, the human rights track record of the end-user and other government actors close to the end-user, whether there is a record of impunity for human rights violations, and whether effective safeguards against abuse exist in the legal framework of the destination country. NSO Group must engage with the end-user and adapt its services and products to mitigate risks. If they determine that their product or their services will be contributing to human rights violations, or if they are unable to mitigate a significant risk of human rights violations, it is incumbent on NSO Group to not undertake the relevant activity. Additionally, NSO Group should take a "human rights by design" approach to the development of its technology, related infrastructure and contractual relationships.[336] Such approach could feature elements such as those highlighted in the report on the surveillance industry by the UN Special Rapporteur on freedom of opinion and expression, including "[i]nternal processes that ensure design and engineering choices incorporate human rights safeguards" and "[r]egular programmes of audits and human rights verification processes."[337]

In September 2019, NSO Group and Novalpina Capital released a Human Rights Policy and a Whistleblower Policy.[338] The content of these policies did not set out how exactly NSO Group would meaningfully ensure that its activities do not cause or contribute to human rights abuses, and raised more questions than they answered. The UN Special Rapporteur on freedom of opinion and expression, then David Kaye, posed a number of questions and concerns to NSO Group on their policies.[339] He stated that NSO Group's human rights policy "neither references the legacy of harm perpetuated as a result of NSO Group's failure to ensure that its technology is used responsibly nor articulates why its new policy will necessarily lead to improved outcomes for victims of surveillance harassment."[340]

While NSO Group responded to these criticisms, it did not provide answers to many of the specific questions posed in the letter.[341] In a follow up letter, the UN Special Rapporteur highlighted that he remained concerned about how NSO Group would ensure protection and remedy for those unlawfully targeted by governments using its technology.[342] In September 2020, Amnesty International wrote to NSO Group regarding the company's External Whistleblowing Policy, requesting details about its internal investigation procedures.[343] In its reply, NSO Group further described how it handles concerns

335. Principle 13, Guiding Principles on Business and Human Rights, www.ohchr.org/documents/publications/GuidingprinciplesBusinesshr_eN.pdf

336. See generally: J. Penney et al., "Advancing Human-Rights-By-Design In The Dual-Use Technology Industry", *Journal of International Affairs*, 20 December 2018, https://jia.sipa.columbia.edu/advancing-human-rights-design-dual-use-technology-industry

337. Report of the Special Rapporteur on freedom of opinion and expression, UN Doc. A/HCR/41/35, para. 60, https://undocs.org/A/HRC/41/35

338. Novalpina Capital, "NSO Group Announces New Human Rights Policy and Governance Framework", 11 September 2019, www.novalpina.pe/nso-group-announces-new-human-rights-policy-and-governance-framework/

339. Letter from the Special Rapporteur on freedom of opinion and expression to NSO Group, 18 October 2019, https://freedex.org/wp-content/blogs.dir/2015/files/2019/10/NSO-GROUP-LETTER-OL-OTH-52.2019-1.pdf

340. See Letter from the Special Rapporteur on freedom of opinion and expression to NSO Group, 18 October 2019, and see NSO Group's response to the UN Special Rapporteur here: https://spcommreports.ohchr.org/TMResultsBase/DownLoadFile?gId=35041

341. See "Answers attributable to an 'NSO Spokesperson'", filed by Mercury Public Affairs, LLC, 18 June 2020, https://efile.fara.gov/docs/6170-Informational-Materials-20200618-467.pdf

342. See: Letter from the Special Rapporteur on freedom of opinion and expression to NSO Group, 20 February 2020, https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL_OTH_20_02_20.pdf

343. Amnesty International letter to NSO Group re: NSO Group internal investigations, 25 September 2020, at Annex 1.

raised regarding misuse of its products.[344] That correspondence reflected additional aspects of the process that are problematic from a human rights perspective, for example, that the company "cannot confirm that any specific concern warranted a thorough investigation or remediation, or whether a user targeted a specific device, which would necessarily confirm the existence of a customer relationship."[345] These exchanges cast in sharp relief the key question of the efficacy of NSO Group's policies in preventing human rights violations.[346]

In line with the UNGPs, *investors* in NSO Group likewise have a responsibility to not cause or contribute to human rights abuses through their investments and to carry out human rights due diligence addressing potential and actual adverse human rights impacts linked to their investments. As part of this responsibility, investors themselves should demand robust transparency about where their investments are channelled, demand relevant data and ensure that surveillance companies themselves conduct adequate human rights due diligence as regards their operations, products and business relationships. This includes meaningfully investigating, remediating and transparently accounting for cases of human rights violations. Indeed, the UN Working Group on the issue of human rights and transnational corporations and other business enterprises has emphasized the importance of investor leverage and investor due diligence in ensuring that companies fulfil their human rights responsibilities.[347] As the Working Group has noted: "Investors can play a significant role in driving wider uptake of human rights due diligence approaches by setting expectations and interacting with the boards and senior executives of the enterprises they invest in."[348] At the same time, investors' human rights due diligence efforts facilitate a broader understanding of investment risk that is crucial to investment decisions, and highlight the importance of access to transparent information on the operation of surveillance companies.

Additionally, Novalpina Capital is a signatory to the Principles for Responsible Investment (PRI),[349] while Oregon State Treasury (which manages the Oregon Public Employees Retirement System,[350] one of the limited partners in the Novalpina Capital Partners I SCSp fund) is a member of the Institutional Limited Partners Association (ILPA).[351] Each of these frameworks recognizes the importance of environmental, social and corporate governance issues in investing.[352] They note the need for transparency on such issues, to investors and, in the case of the PRI, to the public as well.[353] These frameworks further reflect that investors should take proactive measures in ensuring human rights due diligence and transparency, internally and among portfolio companies.

---

344. NSO Group Technologies Ltd. Response to Amnesty International letter re: NSO Group internal investigations, 4 October 2020, at Annex 2; see also NSO Group Technologies Ltd. Response to Amnesty International, Privacy International, and SOMO letter, 2 May 2021, at Annex 4.

345. NSO Group Technologies Ltd. Response to Amnesty International letter re: NSO Group internal investigations, 4 October 2020, at Annex 2.

346. Amnesty International, *Israeli spyware firm NSO must match words with action* (News story, 10 September 2019), https://www.amnesty.org/en/latest/news/2019/09/nso-spyware-human-rights/

347. Report of the Working Group on the issue of human rights and transnational corporations and other business enterprises, UN Doc. A/73/163, paras. 85-91 & 95, https://undocs.org/A/73/163

348. Report of the Working Group on the issue of human rights and transnational corporations and other business enterprises, UN Doc. A/73/163, para. 85.

349. See Principles for Responsible Investment, *Signatory Directory: Novalpina Capital*, www.unpri.org/signatory-directory/novalpina-capital/2456.article

350. See State of Oregon, *PERS Fund/Investments*, www.oregon.gov/pers/Pages/Financials/PERS-Fund-Investments.aspx

351. See International Limited Partners Association (ILPA), *ILPA Member List*, https://ilpa.org/member-list/

352. Principles for Responsible Investment, *What are the Principles for Responsible Investment?,* (n.d.), www.unpri.org/pri/what-are-the-principles-for-responsible-investment; ILPA, *ILPA Principles 3.0,* 2019, pp. 38-39, https://ilpa.org/wp-content/flash/ILPA%20Principles%203.0/?page=38

353. Principles for Responsible Investment, *What are the Principles for Responsible Investment?*, (n.d.), Principles 3 and 6; ILPA, *ILPA Principles 3.0*, 2019, pp. 9 & 38-39.

8. CONCLUSION

The developments in NSO Group's corporate trajectory as documented in this briefing are indicative of the trends and human rights challenges of the surveillance industry at large. NSO Group's corporate structure, fuelled by global investment and shaped by the strategic priorities of private equity firms and governments, has grown to span multiple jurisdictions across the world, including the Britiish Virgin Islands, Bulgaria, the Cayman Islands, Cyprus, Israel, Luxembourg, the UK and the US. NSO Group entities have obtained export licences from Israeli, Bulgarian, and Cypriot authorities.[354] Through multiple layers of holding companies and Novalpina Capital's private equity fund, NSO Group counts as current investors individuals and institutional investors; among them, two public funds in the UK and two in the US. Ultimately, the corporate structure of the NSO surveillance enterprise has facilitated the growth and acceptance of this company and the broader 'intrusion as a service' sector, binding investor returns to ever-expanding surveillance sales. At the same time, NSO Group's longstanding resistance to disclosure concerning its technical offerings, sales, services, human rights impacts or remediation measures has provided the industry a template on how to avoid public transparency and accountability.

This briefing has aimed to address the lack of transparency that is fundamental to the digital surveillance trade by providing a case study of the corporate structure of NSO Group, one of its most prominent participants. It has demonstrated that, in order for governments, investors and civil society to understand and address the human rights risks linked to the industry – and NSO Group specifically – and bring their activities in line with international human rights law and public policy imperatives, transparency is required surrounding, at a minimum, the following three areas:

- *Corporate structure and offerings:* Identifying the participants in the industry, across corporate hierarchies and jurisdictions, is an important step in holding those entities accountable, and understanding which laws apply to their activities. It is also essential to know the purpose or role of each company and what products and services each of those entities offer, to assess relevant export controls and the human rights risks presented.
- *Exports and sales:* Certain detailed information regarding technology and services provided in support of legitimate law enforcement or intelligence operations may understandably be withheld. However, simply identifying countries to which surveillance technology is provided, the identities of the companies providing that technology, and providing aggregate statistics on exports and licence

354. NSO Group Technologies Ltd. Response to Amnesty International, Privacy International, and SOMO letter, 2 May 2021, at Annex 4; see also Columbia Global Freedom of Expression, Case Law: *Malekar v. DECA*, Columbia University, 12 July 2020, https://globalfreedomofexpression.columbia.edu/cases/malekar-v-deca/; Republic of Bulgaria Ministry of Economy, "Публичен регистър на лицата, регистрирани за износ и трансфер на изделия и технологии с двойна употреба [Public register of persons registered for export and transfer of dual-use items and technologies]," http://www.mi.government.bg/files/useruploads/files/exportcontrol/registar_iznos_transfer_22112018.xls, at rows 37 and 61; Novalpina Capital, Response to Open Letter to Novalpina Capital on 18 February 2019, 1 March 2019, www.amnesty.org/download/Documents/DOC10021020 19ENGLISH.PDF.

applications should not be controversial. Such broad categories of information should have no real impact on legitimate operations; rather, impact is likely to take the form of more informed dialogue and greater responsibility in the digital surveillance trade.

- *Company decision-making apparatuses, human rights policies and processes:* Accountability requires understanding which individuals and entities control the activities of the company or otherwise make critical decisions impacting human rights outcomes (for example, board members, owners, etc.). It also requires companies to "know and show" *how* they respect human rights,[355] in order to assess whether commitments align with real practice.

This briefing has collected materials and information relevant to these three categories, in order to support efforts to bring greater transparency and accountability to the digital surveillance trade.

Civil society has worked to promote transparency around the human rights impacts of the surveillance industry, and recognition of its risks is increasing.[356] Robust disclosure and transparency to the public and investors by surveillance companies is an important factor in ensuring accountability and respect for human rights in this industry. Such disclosure is likewise essential to understanding by investors of their own potential linkages to human rights risk. Transparency is equally crucial for individuals to pursue a remedy if they are targeted with surveillance technology in violation of their internationally recognized human rights: individuals must be able to document how the surveillance technology caused or contributed to that violation.

States, surveillance companies and investors all have human rights obligations and/or responsibilities enshrined under international human rights law. In addition, there are a number of legal and regulatory provisions applicable to the industry, such as export controls. However, more effective measures tailored to the specific risks of digital surveillance are necessary to prevent and mitigate human rights abuses facilitated by the products of NSO Group and other industry participants. Without a robust international framework to ensure human rights compliance in the development, sale and use of surveillance technology, it is imperative that governments put human rights safeguards in place. In the interim, they must implement the call by the UN Special Rapporteur on freedom of opinion and expression for an immediate moratorium on the global sale and transfer of the tools of the private surveillance industry until rigorous human rights safeguards are put in place to regulate such practices and guarantee that governments and non-state actors use the tools in legitimate ways.[357]

355. See Principle 15, Guiding Principles on Business and Human Rights, www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

356. L. Parker Deo, "ESG principles prompt lenders to pass on NSO Group loan", *Reuters*, 11 April 2019, https://www.reuters.com/article/esg-nso/esg-principles-prompt-lenders-to-pass-on-nso-group-loan-idUSL1N21T1NP

357. Report of the Special Rapporteur on freedom of opinion and expression, UN Doc. A/HCR/41/35, https://undocs.org/A/HRC/41/35

9. RECOMMENDATIONS

TO STATES:

Immediately:

- Implement a moratorium on the sale and transfer of surveillance equipment until such time as a proper human rights regulatory framework is put in place.
- Adopt and enforce a legal framework requiring private surveillance companies to conduct human rights due diligence in their global operations, supply chains and in relation to the use of their products and services. Under this legislation, private surveillance companies should be compelled to identify, prevent and mitigate the human rights-related risks of their activities and business relationships.
- Adopt and enforce a legal framework requiring transparency by private surveillance companies, including information on self-identification / registration; products and services offered; sales; and human rights due diligence, mitigation and remediation measures; as well as the requirement to produce regular transparency reports reflecting compliance with the UNGPs.
- Disclose information about all previous, current and future contracts with private surveillance companies by responding to requests for information or by making proactive disclosures.

Furthermore, states must, at a minimum, implement the below recommendations if the moratorium on the sale and transfer of surveillance equipment is to be lifted:

- Regulate the export of surveillance technologies, including to:
    a. Ensure the denial of export authorization where there is a substantial risk that the export in question could be used to violate human rights or where the destination country has inadequate legal, procedural and technical safeguards in place to prevent abuse. States should update export control criteria to take into appropriate consideration the human rights record of the end-user as well as the legality of the use of sophisticated surveillance tools in the country of destination, stipulating that applications shall be rejected if they pose a substantial risk to human rights.
    b. Ensure that all relevant technologies are scrutinized for human rights risks prior to transfer as part of the licensing assessment.
    c. Ensure transparency regarding the volume, nature, value, destination and end-user countries of surveillance transfers, for example by publishing annual reports on imports and exports of surveillance technologies. Reform any existing legislation that imposes overly broad restrictions on disclosures of such information.
    d. Ensure that encryption tools and legitimate security research are not subject to export controls.

- Implement domestic legislation that imposes safeguards against human rights violations through digital surveillance, in line with the Necessary and Proportionate Principles, and establishes accountability mechanisms, causes of action, etc. designed to provide victims of surveillance abuses a pathway to remedy.
- Implement procurement standards restricting government contracts for surveillance technology and services to only those companies which adhere to the UN Guiding Principles and have not serviced clients engaging in surveillance abuses.
- Participate in key multilateral efforts (e.g. in support of the UN Special Rapporteur's call for an immediate moratorium on the sale, transfer and use of surveillance technology) to develop robust human rights standards that govern the development, sale and transfer of surveillance equipment, and identify impermissible targets of digital surveillance.

TO SURVEILLANCE COMPANIES:

- Conduct and publicly disclose robust human rights due diligence for all proposed transfers of surveillance technology.
- Refrain from exporting surveillance technology if there is a significant risk of human rights violations by end-users.
- Ensure transparency with regard to sales and contracts.
- Conduct consultations with rights holders in destination countries before signing contracts to identify and assess human rights risks and develop mitigation measures.
- Ensure public commitments to human rights as part of company policy.
- Implement contractual protections against human rights abuses.
- Implement design and engineering choices that incorporate human rights standards and safeguards.
- Ensure regular audits into verification processes, the results of which are publicly disclosed.
- Have an adequate notification process for reporting misuse of technology and grievance mechanisms.
- Implement robust mechanisms for compensation or other forms of redress for targets of unlawful surveillance.
- Adhere to the UNGPs and OECD Guidelines.

TO INVESTORS:

- Institute comprehensive human rights due diligence as part of the pre-investment due diligence process.
- Investigate whether private equity funds under consideration for investment, or other investment vehicles, include or plan to include surveillance companies within their portfolios, and demand notification of any change in investment strategy that might result in investment in such companies.
- Ensure that assets and portfolio companies do not have adverse impacts on human rights, by demanding robust transparency from surveillance companies and by carrying out adequate human rights due diligence before investing in such companies.
- Exercise leverage on portfolio surveillance companies to ensure that the companies implement all the aforementioned recommendations applicable to them.

10. ANNEXES

1. Amnesty International letter to NSO Group re: NSO Group internal investigations, 25 September 2020
2. NSO Group Technologies Ltd. Response to Amnesty International letter re: NSO Group internal investigations, 4 October 2020
3. Francisco Partners Response to Amnesty International, Privacy International, and The Centre for Research on Multinational Corporations (SOMO) letter, 27 April 2021
4. NSO Group Technologies Ltd. Response to Amnesty International, Privacy International, and The Centre for Research on Multinational Corporations (SOMO) letter, 2 May 2021

ANNEX 1

AMNESTY INTERNATIONAL LETTER TO NSO GROUP RE: NSO GROUP INTERNAL INVESTIGATIONS
25 SEPTEMBER 2020

Index number: DOC 10/4186/2020

AMNESTY INTERNATIONAL

AMNESTY INTERNATIONAL INTERNATIONAL SECRETARIAT

Peter Benenson House, 1 Easton Street

London WC1X 0DW, United Kingdom

T: +44 (0)20 7413 5500 F: +44 (0)20 7956 1157

E: amnestyis@amnesty.org W: www.amnesty.org

To NSO Group

E-mail: [redacted]

Cc: [redacted], [redacted]
whistleblowing@nsogroup.com

25 September 2020

RE: NSO GROUP'S INTERNAL INVESTIGATIONS

Dear Mr. Hulio,

We are writing to seek clarity and further information about NSO Group's policies and practices on investigating human rights abuse brought about by the misuse of your company's technology. The purpose of this is to seek information for human rights defenders targeted for surveillance with NSO Group's Pegasus spyware (the "HRDs"), who may wish to pursue remedy from NSO Group for such targeting in line with the right to an effective remedy under international human rights standards such as the UN Guiding Principles on Business and Human Rights (the "Guiding Principles").

The right to effective remedy lies at the core of international human rights law. Companies' responsibility to respect human rights entails enabling access to remedy for adverse human rights impacts with which the business is involved, including where appropriate through effective operational-level grievance mechanisms. We understand that NSO Group intends to offer such a grievance mechanism as detailed in its External Whistleblowing Policy.[1] HRDs who are in contact with Amnesty International may be interested in submitting information about their targeting in order to initiate or further direct investigation and remediation by NSO Group.

Amnesty International remains seriously concerned, however, about the effectiveness of the remediation process as outlined by NSO Group and the potential repercussions for individuals submitting personal identifying information to your company. The External Whistleblowing Policy as written falls far short of standards on remedy required by international law and the effectiveness criteria delineated in the Guiding Principles (Principle 31), most notably with respect to predictability, equitability, and transparency. Indeed, "[p]oorly designed or implemented grievance mechanisms can risk compounding a sense of grievance amongst affected stakeholders by heightening their sense of disempowerment and disrespect by the process." (See Principle 31 Commentary.) If HRDs are to engage with NSO Group regarding human rights impacts, they must have confidence that their efforts and submission of sensitive data will result in real action to remediate harms and prevent future human rights violations.

Amnesty International thus seeks further clarity about NSO Group's practices in investigating human rights abuses linked to its operations. We invite your responses to the following questions:

- In your response to the former UN Special Rapporteur on freedom of expression, David Kaye, dated 21 June 2020, you provide some detail on your company's policy of investigating allegations of misuse. You state, "The Head of Compliance also will review NSO's existing documentation relevant to the allegation. Once all of this information is analyzed, the Head of Compliance, General Counsel, and other high-level Company personnel will evaluate the report and existing information, and determine whether to proceed with a full investigation, as described above, seek additional information, or stop the review, typically because there is not enough information to proceed."

[1] https://www.nsogroup.com/wp-content/uploads/2019/09/External-Whistleblowing-Policy_September19.pdf

Has a thorough and effective investigation been initiated as a result of the information we provided in October 2019 and June 2020 about the targeting of three human rights defenders in Morocco using NSO Group's technology? If yes, please provide details thereof, including information on the progress of any such investigation and remediation action carried out. Further, could you provide information about the criteria under which NSO Group would initiate a thorough and effective investigation after a review, including a detailed description of what NSO Group defines as 'misuse' of its tools?

- If HRDs were to indeed engage with NSO Group in seeking remedy, what specific timeframe will NSO Group commit to in handling and responding to complaints? When can a submitting party expect to hear from NSO Group?

- The External Whistleblowing Policy indicates that only NSO staff would carry out any investigation, raising concerns around a lack of independence and impartiality in the process. Please could you clarify the procedures around conducting an investigation, including how the team of investigators will be appointed? Has the company taken any steps to ensure the grievance mechanism is functionally independent of company operations?

- The Guiding Principles state that any grievance mechanisms undertaken by companies should be transparent. This includes, 'keeping parties to a grievance informed about its progress and providing sufficient information about the mechanism's performance to build confidence in its effectiveness and meet any public interest at stake'. Transparency around how a company addresses its human rights impacts is a key component of human rights due diligence. However, NSO Group's External Whistleblower Policy states, "Due to legal or commercial restrictions you may not be informed of the outcome of the assessment." Will NSO Group inform the submitting party, (1) whether an investigation has in fact been launched, (2) when an investigation has concluded, (3) whether a specified device was in fact targeted with NSO Group technology, (4) whether a specified device was in fact infected through application of NSO Group technology, and (5) whether remedial action was in fact undertaken? As the foregoing questions simply require basic confirmation, is it accurate that confidentiality requirements would not prevent NSO Group from answering? If confidentiality requirements prevent NSO Group from answering the above questions, please provide the specific legal or contractual provisions to the contrary. Additionally, will NSO Group share any details of remedial action it undertakes?

- What steps will NSO Group take to ensure the confidentiality and security of the data shared for the purpose of the investigation? What, if any, information from submitting parties will be shared with state authorities or made public by NSO Group, and what measures are in place to mitigate against potential reprisals by the authorities against the HRD? Will NSO Group provide a written privacy policy detailing its approach?

- Can NSO confirm that seeking or obtaining remedy through the company's grievance mechanism would not preclude HRDs' ability to access remedy through judicial and other state-based mechanisms - for example through the use of legal waivers?

- What specific restrictions will NSO Group seek to impose on submitting parties regarding information shared with them by NSO Group? Please note that, for HRDs who are put under surveillance in violation of their internationally recognized human rights, imposition by NSO Group of restrictions on their ability to publicly acknowledge or seek further remedy for such violation undermines autonomy and compounds the harms suffered.

- We understand NSO Group has the capacity to prevent its technology from targeting devices with certain specified technical criteria.[2] Will NSO Group commit to establishing a "protected list" of the mobile numbers, IP addresses, etc. utilized by HRDs submitting these details, which NSO Group will prevent its

[2] Declaration of Shalev Hulio in Support of Defendants' Motion to Dismiss, *WhatsApp Inc. v. NSO Group Technologies Limited*, https://www.courtlistener.com/docket/16395340/45/11/whatsapp-inc-v-nso-group-technologies-limited/, para. 13; see also, Technology Review (August 2020): https://www.technologyreview.com/2020/08/19/1007337/shalev-hulio-nso-group-spyware-interview/

technology from targeting in the future?

Please note that we may reflect any information we receive from you in our published materials as appropriate. This may include quoting your responses verbatim.

We look forward to receiving your response at your earliest convenience or latest by 6pm on 9 October 2020, by e-mail to Ms. Danna Ingleton ([redacted]).

Sincerely,

Danna Ingleton

Danna Ingleton

Acting Co-Director- Amnesty Tech

ANNEX 2

NSO GROUP TECHNOLOGIES LTD. RESPONSE TO AMNESTY INTERNATIONAL LETTER RE: NSO GROUP INTERNAL INVESTIGATIONS

4 OCTOBER 2020

Index number: DOC 10/4187/2021

October 4th, 2020

VIA ELECTRONIC MAIL

Ms. Danna Ingleton
Acting Co-Director - Amnesty Tech
Amnesty International UK

Dear Ms. Ingleton:

We are in receipt of your letter of September 25, 2020, seeking information with regard to NSO Group's grievance and investigation process. We welcome a continued dialogue with Amnesty International and are pleased to be able to provide further information about our processes and approach.

As you are aware, we develop technologies used by government agencies to thwart terrorist plots, violent crimes, trafficking rings, and other major threats to safety and welfare. We understand that, in the vast majority of instances, our technologies are used lawfully, as intended, and without complaint. However, because of the risk of misuse of our products by third parties, we are committed to the establishment of a human rights program that aligns with the UN Guiding Principles on Business and Human Rights (UNGPs). That includes alignment with UNGP 31, regarding operational level grievance mechanisms.

We also note that no other company in our sector has sought to align its processes with the UNGPs, much less developed a human rights program. As a result, we have limited models from which to draw insights in areas that pose particular challenges and no best practices have been established. Nevertheless, we have and will continue to develop and improve our policies and procedures as our experience unfolds. We believe that our commitment and program is, in fact, best in class and it generally aligns with the newly released U.S. State Department Guidance on Implementing the UN Guiding Principles for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities. We appreciate our continued engagement with Amnesty International UK, along with any constructive recommendations you may be able to offer regarding our approach.

In response to your questions about our whistleblower processes, under NSO's written procedures, when a concern is lodged, we immediately initiate a preliminary investigation. The preliminary investigation process is overseen by an internal committee comprised of the Chief Executive Officer ("CEO"), Chief Product Officer ("CPO"), and General Counsel. This preliminary inquiry is conducted by our Head of Compliance, typically in consultation with independent outside counsel. As part of this process, at the outset, when the circumstances warrant, we will suspend the customer's ability to use our products until the investigation is

concluded. We then seek to determine whether a full investigation is appropriate, which includes an evaluation of whether the concern raised is technically not possible, there is sufficient information to conduct an investigation, or it is otherwise clear that there was no misuse of our System.

Where the allegation appears credible, we launch a full investigation which shall include all or most of the following steps (as the circumstances warrant), engaging with the customer, commissioning reports from third party due diligence providers, performing technical assessments to the extent possible, analyzing relevant domestic legal requirements, and preparing a written summary of the evidence. This process is overseen by a board-level committee, the Governance, Risk and Compliance Committee ("GRCC"), comprised of one independent Director, the Group CEO, the General Counsel and at least two additional directors. Although discretion in appointing the investigative team rests with the GRCC, investigations generally are handled by our internal compliance team in conjunction with independent external counsel, who provides impartial and objective advice and analysis. The internal team typically is led by the Head of Compliance, who reports to the General Counsel, who also reports to NSO's Board of Directors thus ensuring a level of independence when conducting investigations. Where we determine that a customer has misused our system – whether because they have failed to adhere to procedural protections aligned with interpretations of Articles 17 and 19 or the International Covenant on Civil and Political Rights (as construed by the Office of the High Commissioner on Human Rights, the European Court of Human Rights, and others), or appear to have targeted individuals for reasons inconsistent with legitimate aims under those same Articles or under the terms of our agreement – we take immediate remedial action. Such action can range from termination of the agreement, instituting additional protections, and other steps. Indeed, we have terminated agreements and/or or instituted enhanced remedial protections on previous occasions.

We take this process seriously. Every concern that is raised is subjected to it. We neither presuppose the System has been used appropriately or inappropriately, regardless of past allegations or news reports about the customer, or our past relationship. No restrictions are imposed on individuals who submit grievances, including seeking a waiver of rights, confidentiality as to the concern being raised, or to constrain remediation through alternative processes. While our investigations require engagement with our customers and individuals assisting in our investigation process, our investigations are conducted under legal privilege, and we can and do keep the sources of any concerns and materials generated during the investigation strictly confidential. We take all reasonable steps to prevent retaliation against and preserve the rights of privacy of those who report potential misuse of NSO products, although certain identifying information about the alleged target or device must be disclosed in order to conduct an investigation. We also maintain a strict non-retaliation policy embedded in our Whistleblowing Policy and Investigations Procedure. In terms of anticipated timelines, we respond immediately when concerns are raised, and the process normally is completed within 60 days from initiation.

Through this process, we believe that many of the components of UNGP 31 are met. However, because our System is used by authorized governmental parties to thwart major criminal threats and support covert investigations, our engagements – similar to others throughout our sector - are highly confidential. State agencies view that confidentiality as critical to preventing terrorists, criminals and criminal organizations from taking active measures to avoid detection, and thus part of their mission to protect their citizenries from physical harms and material risks.

Accordingly, we can only confirm to submitting parties that their concern is being actively pursued and when it has concluded. Needless to say, the actual government users of our technologies may choose to comment on allegations that are raised, which we often encourage given their greater access to facts, their duty to protect human rights, and their fundamental obligation to ensure that "those affected" by human rights abuses "have access to effective remedy" (UNGP 25). For these reasons, we cannot confirm that any specific concern warranted a thorough investigation or remediation, or whether a user targeted a specific device, which would necessarily confirm the existence of a customer relationship.

We also are conscious that Amnesty International is sensitive to our constraints, as its chapters face similar questions about how much they can keep individuals who lodge concerns apprised of the progress of an investigation, and thus would appreciate any constructive insights you might be willing to share. *See, e.g., Whistleblower Policy*, Amnesty International Australia, Sec. 3.1 (23 July 2019), at https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwi-n--Zu4TsAhWJBhAIHdsCA6cQFjABegQICxAD&url=https%3A%2F%2Fwww.amnesty.org.au%2Fwp-content%2Fuploads%2F2019%2F08%2FBP02-AIA-Policy-Whistleblower.pdf&usg=AOvVaw2QvAofMWQS2W-79Xoam61W).

For the confidentiality, privacy and privilege concerns we have identified, we cannot comment on the substance of the concerns Amnesty International UK raised in October 2019 and June 2020 regarding alleged activities involving the Moroccan government. We can confirm that the information Amnesty International UK provided was taken extremely seriously, subjected to the process identified above, and that our inquiries have concluded. Of course, we cannot confirm who is or is not a customer or whether our products were or were not used in specific circumstances.

Nevertheless, since you requested information in relation to allegations involving the Moroccan government, and while we cannot comment on whether the Moroccan government is a customer or whether our System has been used in any specific circumstance, the Moroccan government itself appears to have responded to allegations Amnesty International has made, at least as reported by the press. Those press reports indicate that the relevant individuals mentioned by Amnesty International in its reports may have engaged in conduct that, it would seem, a state might legitimately investigate

Of course, we welcome any suggestions or insights you have as to how we might provide further details without betraying the customer confidentiality that is absolutely required in our engagements and our sector more generally, and we continue to look for ways to provide greater transparency despite these constraints. We likewise have begun to assess the extent to which we might be able to prevent customers from using our System in relation to certain classes of individuals or entities. We again would welcome any suggestions as to how individuals might practically be identified by name, device or position, and how we might avoid creating an "immunity" for certain individuals that inappropriately exempts them from legitimate government investigations of criminal activity.

We thank you again for your letter, reiterate our desire to engage constructively on these important issues, including about our investigations process and balancing the need for governments to protect their citizens and individual rights to privacy, and look forward to further dialogue.

Sincerely,

Shalev Hulio,
Chief Executive Officer
For NSO Technologies Ltd.

NSO Group Technologies LTD | 22 Galgalei HaPlada St. P.O.B 4166, Hertsliya, 4672222, Israel
Telephone: +972.77.4341292 | Fax: +972.77.4253513 | | Email: office@nsogroup.com

ANNEX 3

FRANCISCO PARTNERS RESPONSE TO AMNESTY INTERNATIONAL, PRIVACY INTERNATIONAL, AND THE CENTRE FOR RESEARCH ON MULTINATIONAL CORPORATIONS (SOMO) LETTER

27 APRIL 2021

Index number: DOC 10/4188/2021

Subject: Francisco Partners Response to Letter of Notification
Date: Tuesday, April 27, 2021 at 9:20:08 AM Eastern Daylight Time
From: Steve Eisner
To: Danna Ingleton

⚠ **CAUTION External Sender** Exercise caution opening links or attachments. Do not provide login details.

Dear Ms. Ingleton:

I am in receipt of your letters dated April 16, 2021 to OSY Holdings Ltd. and to Francisco Partners et al. Below is our response, which I trust you will incorporate into your report. Please confirm receipt by reply email.

***

From March 2014 to March 18, 2019 (the "Sale Date"), Francisco Partners III ("FP III") owned an indirect controlling interest in NSO Group by virtue of its ownership of OSY Holdings Ltd. ("OSY"), which in turn owned a controlling ownership interest in Triangle Holdings, S.A. ("Triangle"). On the Sale Date, OSY disposed of 100% of its ownership interest in Triangle, meaning that Francisco Partners had disposed of 100% of its ownership interest in NSO Group and all subsidiaries and businesses that were in any way related to NSO Group. As part of the sale transaction, Eran Gorev also sold 100% of his ownership interest in Triangle.[1] Thus, following the Sale Date, none of Francisco Partners, FP III, OSY, any other legal entity affiliated with Francisco Partners, nor any individual associated with Francisco Partners (including without limitation Eran Gorev) retained any ownership interest or economic interest in, or other rights relating to, NSO Group or any entity that is in any way related to NSO Group. **For the avoidance of doubt, it is completely false and inaccurate to assert that any individual or entity associated with Francisco Partners, including without limitation Eran Gorev, has any ongoing ownership interest in, ongoing business relationship with, or ongoing influence or control over, NSO Group or any individual or entity associated with NSO Group.** Moreover, since the Sale Date, none of Francisco Partners nor any individual associated with Francisco Partners has any knowledge with respect to the ongoing operations or activities of NSO Group or any of its stakeholders. In addition, since their involvement with NSO Group was purely of a professional nature, each of Eran Gorev, Matt Spetzler and Andrew Kowal resigned from their director roles with NSO Group on the Sale Date.

OSY is a Cayman Islands exempted limited partnership that is wholly owned by FP III. OSY is the holding company through which FP III owned its interest in NSO Group prior to its complete exit from the NSO Group business on the Sale Date as described above. OSY has never exported any products or services, and OSY has not engaged in any activities other than holding ownership interests in Triangle, which interests were completely disposed of on the Sale Date. At this time, OSY has no assets or liabilities and is in the process of being dissolved in accordance with Cayman Islands law.

Francisco Partners GP III is the ultimate general partner of FP III. Neither Francisco Partners GP III nor any other Francisco Partners related entity has ever had any direct ownership interest in Westbridge Technologies, Inc. ("Westbridge").[2] **As described above and for the avoidance of doubt, any indirect ownership interest in Westbridge by Francisco Partners terminated on the Sale Date.** Any registration information that shows Francisco Partners GP III as an immediate owner of Westbridge or shows Francisco Partners GP III (or any other Francisco Partners' entity) as a current owner of any interest in any part of NSO Group is false, inaccurate and unauthorized.

During Francisco Partners' ownership of NSO Group, the technology sold by NSO Group saved tens of thousands of lives, returned kidnap victims to their loved ones and assisted government agencies in apprehending the world's most notorious criminals. Nonetheless, prior to making its investment, Francisco Partners recognized that NSO Group sells sensitive technology that has a risk of being misused. That is why Francisco Partners insisted on implementing a variety of controls in the business, including without limitation the creation of the Business Ethics Committee (BEC) consisting of independent experts that reviewed all potential sales and addressed alleged cases of misuse. Under Francisco Partners' ownership of NSO Group, the BEC blocked tens of millions of dollars in sales that would have otherwise been permitted based on applicable legal requirements.

Francisco Partners' limited partners are not involved in investment decision making and are not provided information regarding Francisco Partners' investments in advance of such investments being made. Francisco Partners' individual professionals serve on the Board of its portfolio companies, where they are responsible for working with each company's management team to set the company's strategic direction. Day-to-day decision-making, including how to respond to press inquiries, falls within the purview of a company's management team and not with the Francisco Partners' individuals who serve on that company's board of directors.

———————

1. During FP III's ownership of Triangle, for structuring purposes, Eran Gorev held a small ownership interest directly in Triangle. Such ownership interest was also sold on the Sale Date as part of the transaction pursuant to which FP III sold its interest in NSO Group, and Eran Gorev ceased to have any ownership interest in NSO Group and any business associated with NSO Group as of the Sale Date.

2. Westbridge is or was an operating subsidiary of NSO Group. During FP III's ownership period, FP III's interest in Westbridge (and therefore any interest attributable to FP III's ultimate general partner) was held indirectly through OSY and Triangle. Neither Francisco Partners, nor any individual associated with Francisco Partners, has any knowledge whatsoever as to the corporate structure of NSO Group post the Sale Date.

***

Sincerely,

Steve Eisner
Partner, General Counsel and Chief Compliance Officer
Francisco Partners
One Letterman Drive | Building C - Suite 410
San Francisco, CA 94129
Mobile [redacted]
Direct [redacted]
Fax [redacted]

[1] During FP III's ownership of Triangle, for structuring purposes, Eran Gorev held a small ownership interest directly in Triangle. Such ownership interest was also sold on the Sale Date as part of the transaction pursuant to which FP III sold its interest in NSO Group, and Eran Gorev ceased to have any ownership interest in NSO Group and any business associated with NSO Group as of the Sale Date.

[2] Westbridge is or was an operating subsidiary of NSO Group. During FP III's ownership period, FP III's interest in Westbridge (and therefore any interest attributable to FP III's ultimate general partner) was held indirectly through OSY and Triangle. Neither Francisco Partners, nor any individual associated with Francisco Partners, has any knowledge whatsoever as to the corporate structure of NSO Group post the Sale Date.

Please refer to the following link for important Francisco Partners disclaimer information regarding this e-mail communication: www.franciscopartners.com/us/email-disclaimer. By messaging with Francisco Partners you consent to the foregoing.

ANNEX 4

NSO GROUP TECHNOLOGIES LTD. RESPONSE TO AMNESTY INTERNATIONAL, PRIVACY INTERNATIONAL, AND THE CENTRE FOR RESEARCH ON MULTINATIONAL CORPORATIONS (SOMO) LETTER

2 MAY 2021

Index number: DOC 10/4189/2021

May 2, 2021

Ms. Danna Ingleton
Deputy Director, Amnesty Tech
Amnesty International UK

Ms. Roberta B. Cowan
Senior Researcher,
Centre for Research on Multinational Corporations (SOMO)

Dr. Ilia Siatitsa
Programme Director and Legal Officer
Privacy International

Dear Ms. Ingleton, Ms. Cowan and Dr. Siatitsa:

We received your five letters dated April 16, 2021 (the "Letters"), seeking information about legal entities and individuals named in your forthcoming report regarding the "corporate structure of ... NSO Group" (the "Report"). We appreciate this continued dialogue with Amnesty International and welcome the new dialogue with SOMO and Privacy International. We are pleased to provide our preliminary observations followed by responses to your specific questions.

As we have made clear, we are committed to promoting transparency wherever possible and are currently in the process of drafting our first transparency report, consistent with our commitment to responsible business practices, which we intend to issue by June 2021. At least some of the questions you pose will be answered in that report. Nonetheless, we are pleased to provide you with insight into this information and respond to the issues that you have raised. While it appears that you may have spent some time gathering the information that forms the basis of the questions, in the future, it may be more efficient simply to ask us for it.

Our answers to your questions appear below. By way of introduction, as you are aware, while our corporate mission is to create technologies to help government agencies prevent and investigate terrorism and crime – to save lives – we are aware of the risk of potential misuse of our products. This is why we have designed a human rights program that seeks to align with the UN Guiding Principles on Business and Human Rights (UNGPs) to the maximum extent feasible. While we believe we have the leading program in our sector, we are committed to continuous improvement, including through ongoing engagement with Amnesty International, SOMO, Privacy International and other stakeholders. We also call on others in the field to do the same, and develop in collaboration with a range of experts best practices in this field.

In addition to the requirements of our own program, we also face close scrutiny from Israel's Defense Export Control Authority. We are aware, of course, that Amnesty International has questioned and

sought to challenge its compliance approach. However, a recent decision by the Tel Aviv Administrative Court confirmed:

> *....that the process of supervising and processing applications for marketing and/or defense export licenses is a sensitive and rigorous process, in its framework the export applications are reviewed in depth by the various security authorities that deal with the various security and diplomatic aspects, as well as technological and other aspects. Licensing is done after a very strict process, and after the license is granted, the Authority conducts close supervision and monitoring, and if necessary, and if it is found that the use of the license conditions is violated, especially when there are violations human rights, they take action to revoke or suspend the defense export license…*
>
> *I am satisfied that Respondents 1-4 do their job very prudently before a marketing and/or export license is granted and also after it is granted the holder of the license is subject to close monitoring by DECA, which shows a particularly high sensitivity to any violation of human rights.*

Administrative Petition 28312-05-19, Malka et al. v. The Head of the Defense Export Control Authority et al. We raise this not to suggest that the oversight and processes associated with our products cannot be improved, but as a gentle reminder that our internal frameworks supplement an "in depth" legal regulatory one.

With respect to the references to previously reported, alleged misuse included in the Report, we have responded to you in each instance at the time that you raised your allegations. We will not repeat each of our responses at this time.

Organizational Structure

As you noted, the organizational structure of our company has resulted from various acquisitions, investments and mergers. This was never intended to be used as a shield to hide our corporate identity for any nefarious or other reason but rather reflects the reality of growth through acquisitions. For clarity in this letter, when we refer to the "Group" we are referring to the whole group of companies in the corporate structure beginning with Triangles Holdings SA.

Grievance and Investigation Process

As we previously shared with you (please see our letter to you dated October 4, 2020), under NSO's written procedures, when a concern is lodged, we immediately initiate a preliminary investigation. This preliminary inquiry is led by our Vice President, Compliance, typically in consultation with independent outside counsel. As part of this process, at the outset, when the circumstances warrant, we will suspend the customer's ability to use our products until the investigation is concluded. We then seek to determine whether a full investigation is warranted.

Where the allegation appears credible, we launch a full investigation. This process is overseen by a board-level committee, the Governance, Risk and Compliance Committee ("GRCC"). Where we

determine that a customer has misused our system, or appears to have targeted individuals for reasons inconsistent with legitimate aims under international human right norms – which is required under the terms of our agreement – we take immediate remedial action. Such action can range from termination of the agreement, instituting additional protections, and other steps.

We take this process seriously and follow this process in connection with every concern that is raised. We do not seek any restrictions on individuals who submit grievances, including seeking a waiver of rights, requesting confidentiality as to the concern being raised, or constraining remediation through alternative processes.

Responses to the Letters

We also provide the following, consolidated responses to the questions raised in the Letters:

1. The shareholders of NSO Group Technologies Ltd. are Q Cyber Technologies Ltd. and NSO Group Technologies Ltd. itself. Under Israeli law a company may hold its own shares in various instances (such as a buyback). As a result, the full ownership rights of NSO Group Technologies Ltd. are held by Q Cyber Technologies Ltd. (Please see the attached extract from Israel's Companies Registrar).

2. There is currently no relationship between Westbridge and Francisco Partners. The ownership of Westbridge was acquired as part of the transaction between Novalpina and Francisco Partners in 2019. The current CAGE registration information is incorrect. Thank you for bringing this to our attention. We shall act to correct this.

   In the United States, our marketing activities are focused on all legitimate *governmental* users for our Group products in accordance with local laws. Due to various confidentiality constraints we cannot provide specific details, if any, about customers in the US. With respect to the terms referred to in your question "Q Suite" and "Phantom," these are not terms that the Group currently uses in its marketing activities. Moreover, we cannot state with certainty what a former employee meant by their use of the term "Q Suite." We assume, probably like you, that this former employee was referring to the various technologies marketed by the Group as they pertain to the market in the United States. Based on the language of the brochure, it would seem that Phantom was a marketing name given to a version of Pegasus at some period of time.

3. As a shareholder, Novalpina appoints members to the Group Boards of Directors for Triangle Holdings S.A. and OSY Technologies S.a.r.l. and various committees of those boards, each of which provides strategic direction regarding the activities of the Group. Novalpina is not involved in the day to day, operational activities of the Group, which is the responsibility of Group management. As with any corporation, senior management may consult from time to time with members of the Board on various matters, but Board members are not involved directly in day to day activities.

4. Group products are exported in accordance with all applicable export regulations and relevant export authorities, including Israel's Defense Export Control Law ("DECL"). Group entities export products from Israel, Bulgaria, and Cyprus, and their respective export control authorities.

   We do not maintain statistics related to the percentage of licenses denied because we do not believe this provides much insight into our activities. The percentage of licenses denied does not reflect the number of countries where we will not sell Group products (i) based on our internal policies or (ii) because we know that the relevant authorities will not authorize an export license. Moreover the percentage of licenses denied could be skewed by the overall number of requests, ranging from a 50% denial rate if only one of two requests is denied as compared to a 5% denial rate if one of twenty requests is denied. However, although we do not have statistics, we confirm that export authorities in Israel, Cyprus and Bulgaria have denied Group applications for export licenses.

   Q Cyber Technologies SARL acts as a commercial distributor for the products of the Group companies, as such it signs contracts, issues invoices and receives payments from Group customers. These activities are the basis for reported income. Revenues are recognized in accordance with Generally Accepted Accounting Principles and audited by a leading global auditor. Q Cyber Technologies SARL does not export Group products and has not sought an export license in Luxembourg.

5. The GRCC is comprised of one independent Director, the Group CEO, and at least two additional directors, one of whom is the Group General Counsel. There is no specific or additional compensation for GRCC members. Neither the executive members or board members receive any compensation beyond their existing compensation from the Group.

   The Board of Directors of OSY Technologies SARL appoints the GRCC. The GRCC is responsible for approving, monitoring and reviewing the Group's policies regarding governance, risk and compliance, as well as having a veto right on certain of the Group's business opportunities, including the Group's products and services, in accordance with the Human Rights Due Diligence Procedure and overseeing the Group's adherence to our corporate social responsibility principles. The GRCC advises every company in the Group, including, but not limited to IOTA and its subsidiaries.

   The Group obtains advice on Human Rights issues from a group of internationally recognized advisers that have significant experience in the fields relevant to our activities. Further details on these matter shall be provided in our Transparency Report.

   GRCC members have significant and varied experience and expertise. Our General Counsel has been a General Counsel of large defense corporations for over three decades, is an expert on International Law, has over a decade experience in compliance, and is recognized as one of Israel's leading authorities in this field. Another board member on the GRCC is a founder of a leading provider of AML services, and has many years of compliance experience. The independent director brings many years of high level experience to the GRCC.

6. CT-Circles Technologies Ltd. is not part of the Group. We do not have any details regarding this entity.

7. ESOP is a company that held shares and options on behalf of employees of the company as part of the Company's Employee Stock Ownership Plan. Applicable tax regulations require establishment of such an entity in order for the Employee Stock Ownership Plan to meet the requirements for tax benefits.

8. The board of directors of Triangles and its committees meet on a monthly basis to discuss various matters, including matters related to the strategic direction of the Group and regulatory affairs, in accordance with the Triangle Holdings Article of Association. In particular, the Triangles Board adopted various procedures for the implementation of the Group's Human Rights Policy, including the Human Rights Due Diligence Procedure and Product Misuse Investigation Procedure and periodically discusses human rights issues related to the group's activities. The GRCC, which as stated above is a committee of the OSY Board of Directors, meets on a monthly basis and its discussions relate to the human rights issues of the group's activities.

9. NSO Group companies engage in the following activities:

    - NSO Group Technologies Ltd. and Q Cyber Technologies Ltd. develop, market and export Pegasus and related analytical products for governmental use. In addition, these entities provide certain sales, marketing services and other administrative support and oversight to their respective affiliates.

    - Convexum develops and exports the Eclipse anti-drone system.

    - Wayout develops cyber security products for the IoT world for governmental use.

    - The IOTA part of the Group is currently headquartered in Cyprus. Operations are conducted, under contract with the Group's Bulgarian entities, in Bulgaria.

    - The Bulgarian companies provide, on a contract basis, research and development services to their respective Cypriot affiliates and export the network products for governmental use.

    - None of the other Group companies currently develop or export products.

10. NSO Group Technologies Ltd., Q Cyber Technologies Ltd., Convexum, Wayout, and the Bulgarian companies export products and obtain licenses from their relevant export authorities for all of the products that require export licenses.

11. The Group's relationships with the following are:

    - Shalev Hulio, Omri Lavi, Yuval Somekh and Asher Levy are directors in the Group. Director responsibilities are described above.

- Kevin Wilson is a former employee and current shareholder in Triangle Holdings, with no other position in the Group.

- Niv Carmi is no longer affiliated with the Group.

- Gaetan Dumont is a professional director in 5 of the 8 Luxembourg companies of the Group. Dumont holds no other position in the Group.

- Alexei Voronovitsky is a former consultant that no longer holds shares in any Group company and holds no other positions with the Group.

12. NGTP and Sesame are currently inactive. They were created for potential future plans of the company that have not currently materialized. Emerald and Diamond are companies created for the sake of granting stock options to management, directors and employees under stock option plans.

    Magnet Bulgaria is currently dormant and inactive. Its registration with the Export Control Authority in Bulgaria expired in 2020 and was not renewed. It has never received licenses for the export of either Vole or Pixcell.

    OSY Holdings is a company through which Francisco Partners previously held shares in the group. It is no longer related to the Group and we have no information about its directors or activities.

    The Group has no companies located in Cayman Islands or the British Virgin Islands. OSY Holdings Ltd. and Global Seven Group LP have no shares or other interest in Triangle Holdings.

We thank you for your letter and reiterate our commitment to transparency and the UNGPs, and we welcome the opportunity to engage constructively on these issues.

Sincerely,

Chaim Gelfand
Vice President, Compliance
NSO Group

AMNESTY INTERNATIONAL IS A GLOBAL MOVEMENT FOR HUMAN RIGHTS. WHEN INJUSTICE HAPPENS TO ONE PERSON, IT MATTERS TO US ALL.

CONTACT US

info@amnesty.org

+44 (0)20 7413 5500

JOIN THE CONVERSATION

www.facebook.com/AmnestyGlobal

@amnesty

OPERATING FROM THE SHADOWS

INSIDE NSO GROUP'S CORPORATE STRUCTURE

Targeted surveillance is a serious threat facing human rights defenders globally. Though often carried out by states, this practice is enabled by digital surveillance tools provided by private companies. However, the lack of transparency about the operations of the surveillance industry poses a serious obstacle for victims of unlawful surveillance to seek accountability and the right to remedy. This briefing seeks to shed light on one specific company – NSO Group – and thereby help to overcome this barrier.

This briefing is jointly written by Amnesty International, Privacy International and The Centre for Research on Multinational Corporations (SOMO) to detail the complex corporate structure of NSO Group – how it has changed over time and continues to change, reflecting the evolution and effects of private sector participation in state surveillance.

SOMO

PRIVACY INTERNATIONAL

AMNESTY INTERNATIONAL