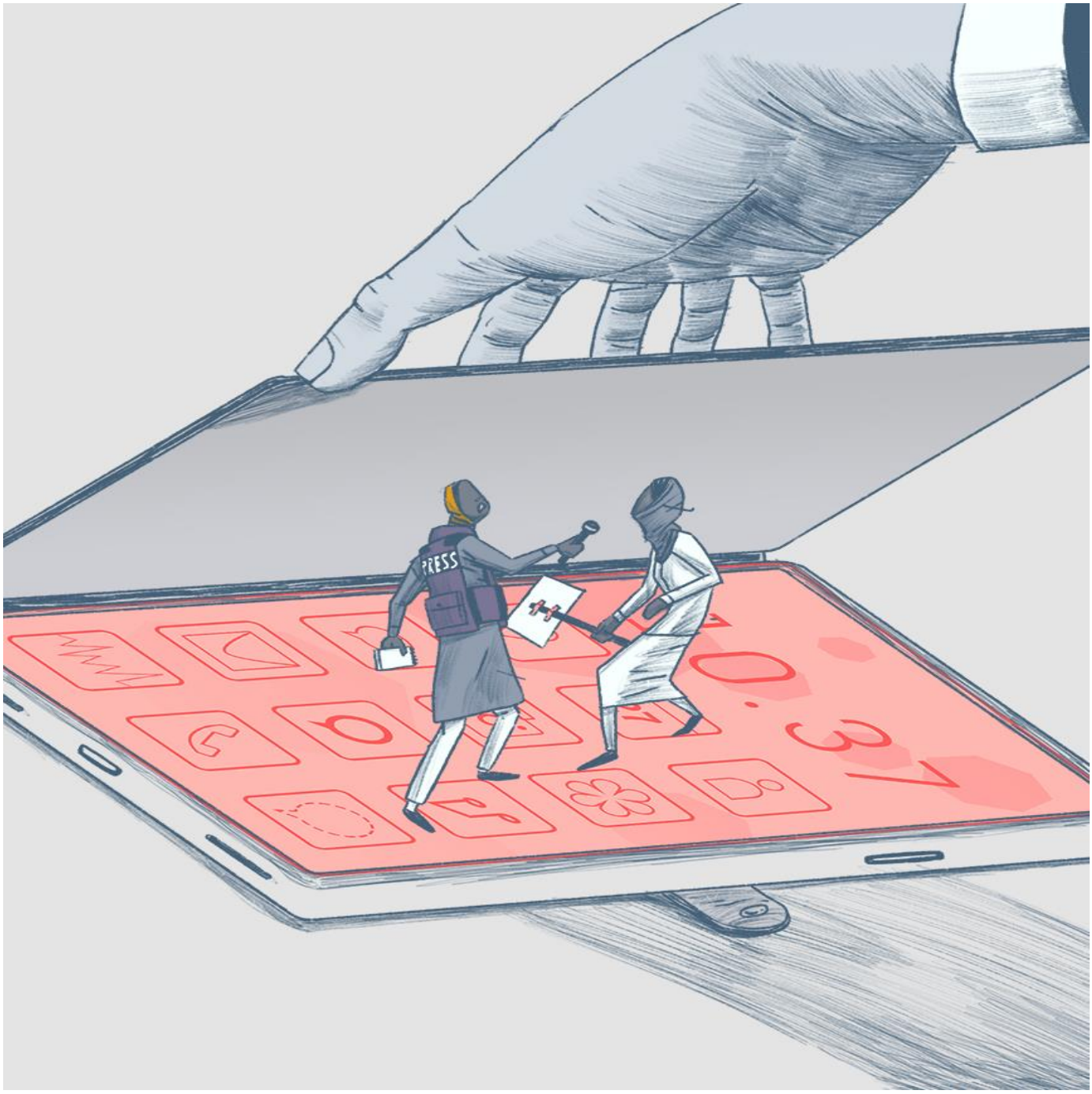

OPERATING IN THE SHADOWS

INVESTOR RISK FROM THE PRIVATE SURVEILLANCE INDUSTRY

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.

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

Index: DOC 10/4359/2021
Original language: English

amnesty.org

Cover photo: *Howie Shia*

AMNESTY INTERNATIONAL

CONTENTS

1. INTRODUCTION

Many states enhance their surveillance capabilities by buying spyware or other digital surveillance tools from surveillance companies. While governments claim to use such products to fight crime and terrorism, many have used them to target human rights defenders (HRDs), activists, journalists and members of civil society in violation of their internationally recognized human rights. This is done by attempting to, and in many cases successfully compromising their digital devices in order to monitor their activities and communications and obtain access to their private data. Such targeted digital surveillance is ultimately used to harass, intimidate, and persecute those targeted. It has led, in some cases, to a variety of human rights violations and abuses, including arbitrary detention and torture.[1]

The UN Special Rapporteur on Freedom of Opinion and Expression (the UN Special Rapporteur) concluded in 2019 that the surveillance industry continues to provide its services "unsupervised and with something close to impunity."[2] This finding was based on years of evidence-gathering that has consistently demonstrated 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 the global targeting of HRDs, journalists and many others with software from NSO Group Technologies Ltd. (NSO Group) as was revealed in the Pegasus Project in July 2021.[4]

Targeted digital surveillance includes a range of tactics and technologies. This briefing focuses on government hacking – when authorities compromise a targeted person's devices, often by exploiting system or software vulnerabilities to install malware and spyware. It examines the role of the global surveillance industry in government hacking and allegations of involvement in human rights violations. Amnesty International believes that existing regulatory safeguards are inadequate and ineffective in preventing or mitigating human rights abuses facilitated by the digital surveillance industry. This briefing outlines the material risks, including reputational, financial, and legal risks facing companies and investors in this sector. It uses the surveillance company NSO Group as a case study, as the company and its functioning exemplify the risk that the poorly regulated surveillance industry poses. Given the scale of disclosures revealed in the Pegasus Project, there is an urgent need for investors to assess risk of investments in the private surveillance industry. In this briefing, we suggest questions for investors and potential investors to ask investment managers and surveillance companies in order to understand whether these risks and impacts are being adequately assessed, prevented, mitigated and managed (Section 7). This briefing accompanies a publication entitled, 'Operating from the Shadows: Inside NSO Group's Corporate Structure', which examines the corporate structure of NSO Group in more detail.[5]

THE FOLLOWING HAVE BEEN IDENTIFIED AS THE MAJOR HUMAN RIGHTS AND MATERIAL RISKS FOR INVESTORS

- Contributing to or being directly linked to human rights abuses
- Revenues reliant on exploitation of widely used digital platforms offered by major technology companies
- Litigation risk against portfolio companies
- Legal risk due to non-compliance with new regulation and evolving government norms.

2. THE SURVEILLANCE INDUSTRY

The main purpose of the surveillance industry is the enablement, for profit, of state intelligence and security apparatuses. Targeted digital surveillance, which includes government hacking,[6] is increasingly used by governments to crack down on human rights defenders.[7]

Government hacking is in many cases enabled by the spyware of private surveillance companies like NSO Group.[8] This spyware enables the access, collection and analysis of highly personal data.[9] Government 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. Government hacking is not simply a passive technique of interception; it can be used to substantively interfere with individuals' lives. Exploitation of computer systems' 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. In addition to the sale of surveillance tools, private surveillance companies may also play a continued role in advising state actors on the operation of their spyware and other products.[10]

The legality of states' use of this surveillance technology is far from clear. As explained by the UN Special Rapporteur: *"It is insufficient to say that a comprehensive system for control and use of targeted surveillance technologies is broken. It hardly exists..."*[11]. Moreover, a legal basis for permitting a private company to develop and trade in digital surveillance technology has never been adequately spelled out. 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, the current regulatory lacuna increases the risk that technology will be misused with potential financial and reputational consequences for spyware companies and investors. As pressure from civil society and regulatory bodies builds to urgently fill these legal gaps, the private surveillance industry faces a period of regulatory flux. Investors should track these regulatory developments. These could result in limitations on their operations in the future.

Material risks to investors due to exposure to this sector might arise in a number of ways. Some large companies that offer a range of products and services beyond surveillance tools are publicly traded. Many others are backed by private investment. For example, NSO Group is currently majority owned by a private equity firm – Novalpina Capital – in which some pension funds have invested.[12] According to recent reports, NSO Group is considering becoming a public company either via an initial public offering or a merger with a special purpose acquisition company (SPAC).[13] In addition, media reports reveal that Novalpina Capital plans to liquidate following an internal dispute,[14] and NSO Group are reportedly in talks to transfer management of that fund to a US consulting firm.[15] It is currently unclear what the motivation of these changes are or whether these reported changes will come to fruition.

While investors will have varying degrees of influence over a company depending on the nature of the investment, they can each take steps to mitigate the risks identified in this briefing. Those who invest via private equity firms can establish investment strategy criteria that limit their exposure to the sector without explicit approval prior to investment. Likewise, asset owners concerned about potential exposure to this sector via public listings should engage with their fund managers to understand whether risk can be avoided. Investors with ownership rights of voting and engagement can attempt to influence a company, for example, by requiring robust transparency and human rights due diligence from private surveillance companies.

Due to secrecy and confidentiality requirements, it is questionable whether an industry dependent on governments – including those who routinely clamp down on human rights – as its customer base can or will ever provide the appropriate disclosures to enable investors to identify and assess risks. The questions in this briefing are intended to help investors evaluate whether it is possible for them to understand the degree of risk to which they are exposed from investments in the private surveillance industry.

3. RISK OF CONTRIBUTING TO OR BEING DIRECTLY LINKED TO HUMAN RIGHTS ABUSES

Digital surveillance products and services of the type sold by NSO Group are considered 'dual use', meaning they can be used for both civilian and military purposes without modifications. Numerous civil society groups and journalists have documented how targeted surveillance technologies manufactured by surveillance companies are misused to target civil society. This exposes investors to the risk of being directly linked to human rights abuses and of possibly even contributing to them. This increases their material risk, including the risk of litigation and reputational damage.

For example, 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,"[16] the track record of deployment suggests otherwise.

.

UNLAWFUL SURVEILLANCE VIOLATES 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 protected by both the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). The ICCPR upholds the right to hold opinions without interference[17] and guards against arbitrary and unlawful intrusion on privacy.[18] International law and standards also require that any interference by the state on the right to privacy should be lawful, necessary, proportionate and legitimate. The targeting of HRDs with digital surveillance technology solely because of their human rights work is unambiguously unlawful under international human rights law.[19]

In July 2021, the Pegasus Project, a collaborative investigation that involved more than 80 journalists from 17 media organizations in 10 countries coordinated by Forbidden Stories with technical support from Amnesty International, revealed to the public just how states' use of the targeted digital surveillance tools supplied by one of the industry's most prominent participants is utterly out of control, destabilizing, and threatening to individuals' human rights, including their physical safety. The investigation revealed that

human rights defenders, journalists, lawyers, activists and politicians across the globe have been targeted on a massive scale.[20]

From the leaked data and their investigations, Forbidden Stories and its media partners identified potential NSO clients in 11 countries: Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, Togo, and the United Arab Emirates (UAE).

The Pegasus Project revelations have added to a mounting pile of evidence of human rights violations uncovered over the years by researchers, journalists, activists resulting from the unchecked use of NSO Group's technologies. A full list of individuals impacted is beyond the scope of this briefing, however, investors should note that these revelations disprove any claims by NSO that such attacks are a rare or anomalous use of their technology. While the company asserts its spyware is only used for criminal and terror investigations, it has become clear that NSO Group's technology facilitates systematic abuse, in which NSO Group appears to be complicit.[21]

While NSO Group has claimed that it wishes to engage with civil society about allegations that it has contributed to human rights abuses, the company has at the same time repeatedly rejected evidence presented by civil society of such abuses,[22] casting doubt over the sincerity of its claims.

These revelations are the tip of the iceberg, and new cases of unlawful targeted surveillance continue to come to light. Given the secrecy associated with targeted digital surveillance, and NSO Group's strong resistance to providing any details of its sales (including who it sells to) or efforts to prevent and address misuse of its technology, this record likely represents a window into a much larger phenomenon.

3.1 HUMAN RIGHTS ABUSE – AN INTEGRAL FEATURE NOT A BUG OF THE DIGITAL SURVEILLANCE INDUSTRY.

NSO Group is not the only company linked to human rights abuse. A number of surveillance technology companies have also been implicated, demonstrating an industry-wide pattern of conduct that threatens human rights.

- Remote Control System (RCS), a computer spyware marketed and sold exclusively to governments by Italian company Hacking Team, was used against journalists and human rights activists in Morocco [23] and the United Arab Emirates.[24]
- FinSpy, a surveillance software suite produced by Finfisher, was used to target HRDs and civil society in many countries, including Bahrain,[25] Turkey,[26] and the US.[27]
- Communications interception equipment and annual support services was provided from March 2015 to February 2017 by Israeli Verint Systems Ltd, a subsidiary of American Verint Systems Inc., through Vivacell Network of the World, to the South Sudanese authorities. This is concerning because both South Sudan's legal framework governing surveillance and the Israeli export licensing regime in practice are not in line with international human rights standards.[28]
- Four executives of surveillance companies Amesys and Nexa Technologies were indicted by a Paris Court for complicity in torture over the sale of surveillance technology to governments in Libya and Egypt.[29]

3.2 LACK OF TRANSPARENCY

Transparency is another problem facing this industry. NSO Group exemplifies this because the lack of information around NSO Group's corporate structure, the jurisdictions within which it operates and the opacity in its contracts with governments. While, Amnesty International's report on NSO Group's corporate structure did shed light on some of this information, there continues to remain a lack of transparency. This coupled with the scale of deployment of its products, and concerns about the adequacy of its due diligence and remediation efforts all pose significant barriers for governments, investors and civil society seeking to understand and address the human rights risks linked to NSO Group's products and services. NSO Group has sought to make itself 'transparency-proof' on numerous aspects of its operations, citing Israeli legal requirements and client confidentiality.[30]

Since 2019, civil society has exchanged a series of letters and communications with NSO Group and its majority owner – the private equity investor Novalpina Capital. In that correspondence Novalpina made a number of commitments regarding NSO Group's compliance with and implementation of the United Nations Guiding Principles on Business and Human Rights (UN Guiding Principles).[31] Many of these promises remain outstanding and unaddressed over two years later. Nothing has been presented by NSO Group or Novalpina Capital that permits an objective evaluation of whether there is meaningful implementation of the UN Guiding Principles.[32] In June 2021, NSO Group released its first transparency report.[33] This report was yet another missed opportunity for the company to be transparent and provide meaningful information about the human rights impacts of its products.[34] For example, in the report, NSO Group ignored the issue of remediation for victims and failed to disclose all the legal challenges the company has faced resulting from the misuse of its technology. This is a serious omission that leaves investors in the dark about the legal risks they may face.[35] In response to the Pegasus Project revelations, NSO Group refused to engage with media queries, choosing opacity when confronted with human rights violations perpetrated by states believed to be its clients.[36]

Actual and potential investors in private surveillance companies would benefit from greater transparency of information crucial to understanding investment risks and impacts, and fulfilling their own responsibilities and commitments to respect human rights. This would enable them to make more informed investment decisions.

3.3 LICENSING REGIMES ARE NOT ENOUGH TO PREVENT HUMAN RIGHTS VIOLATIONS

Investors should not solely rely on the fact that exports of surveillance products are licensed by government agencies as an indication of the lawfulness of the products and their use. Depending on the national legal framework in the country 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 economic interests, industry growth or perceived geopolitical influence weigh in favour of licence approval.[37]

As noted by the UN Special Rapporteur, the global export control framework governing surveillance technology and its national implementation are inadequate when it comes to regulating such technology or accounting for its human rights impacts.[38] Even while exports may be "licensed", they could still present a grave risk to human rights, especially in countries where the legal framework governing the use of such technology is inadequate.

For example, NSO Group confirmed in correspondence with Amnesty International 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".[39] However, in Israel, human rights considerations are not referenced in the Defence Export Control law[40] and there is no information available on how extensively and appropriately Israel's human rights obligations are considered in making licensing determinations. While regulation in other jurisdictions from which NSO Group exports such as the EU (Bulgaria), includes human rights criteria in the licensing assessments, documentation by media and civil society groups suggests that in general human rights considerations are not decisive criteria in those licensing decisions (albeit complete information about destination countries and products exported are unavailable).[41]

3.4 NSO GROUP'S RESPONSIBILITY TO RESPECT HUMAN RIGHTS

The UN Guiding Principles[42] 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 UN Guiding Principles provide the framework within which participants in the digital surveillance trade can work to fulfil their responsibility to respect human rights, and prevent, mitigate, and remedy actual and potential adverse human rights impacts. The Organisation for Economic Co-operation and Development (OECD) has provided a practical guide for how such due diligence should be carried out through its OECD Due Diligence Guidance for Responsible Business Conduct (OECD Due Diligence Guidance). As set out in these international standards, an important step in a company's due diligence process is accounting for how they address their impacts on human rights. Once a company has assessed the actual and potential negative human rights impacts, it should act upon those findings by preventing harms or mitigating risks, tracking and monitoring the action taken to address the human rights risks and abuses and communicating what steps the company has taken to address them, including by reporting publicly. By doing so, these corporate entities will allow for independent scrutiny of their business conduct and also reduce their own legal, financial, and reputational risks. However, the industry's current due diligence with respect to human rights is totally inadequate, which in turn creates risks for investors. [43]

Indeed, the repeated abuse of NSO Group's tools to unlawfully target activists and its failure to publicly account for how it is addressing the actual and potential human rights impacts of its products and services demonstrate that NSO Group's policies and practices in preventing human rights abuses are ineffective.[44]

In September 2019, NSO Group and Novalpina Capital released a Human Rights Policy and an External Whistle-blowing Policy.[45] 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. The UN Special Rapporteur posed a number of questions and concerns to NSO Group on their policies.[46] While NSO Group responded to these criticisms, it did not provide answers to many of the specific questions posed in the letter.[47] 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.[48] In particular, he requested that NSO Group provide specifics of the due diligence it carries out to determine whether the end-user actually uses the technology in a manner consistent with human rights

law, examples of where , as it has claimed, determined that the conduct of a client constituted a material breach and the actions taken by NSO Group, and to provide information on how it differentiates a genuine concern from a malicious claim under its Whistle-blowing Policy.

In September 2020, Amnesty International wrote to NSO Group regarding the company's External Whistle-blowing Policy, requesting details about its internal investigation procedures. In its reply, NSO Group further described how it handles concerns raised regarding misuse of its products. That correspondence detailed additional aspects of the process that are problematic from a human rights perspective. For example, the company invokes client confidentiality in stating that it "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."[49]

NSO Group's responses to both the Special Rapporteur and those sent to Amnesty International raise serious concerns about the efficacy of NSO Group's human rights due diligence practices in actually preventing human rights abuses. Nothing has been presented by NSO Group or Novalpina Capital that demonstrates that there is meaningful implementation of the UN Guiding Principles. This makes it impossible to independently assess NSO Group's due diligence policies and practices and whether they have taken and are taking adequate steps to identify, prevent, mitigate and address human rights risks and abuses and ensure they do not cause or contribute to abuse.[50] Indeed, the Pegasus Project identified numerous instances of unlawful targeting after the publication of the company's human rights and whistle-blowing policies.

3.5 INVESTORS' RESPONSIBILITIES UNDER THE UNITED NATIONS GUIDING PRINCIPLES ON BUSINESS AND HUMAN RIGHTS

Under the UN Guiding Principles investors likewise have a responsibility to not cause or contribute to, or be directly linked to, human rights abuses through their investments.[51] Investors should carry out human rights due diligence to identify, prevent, mitigate and account for how they address potential and actual adverse human rights impacts linked to their investments.[52] 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.[53] 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."[54] Failing this, investors run the risk of contributing to, or being directly linked to human rights abuses. For example, Amnesty International has determined that certain state pension funds which have a stake in NSO Group are directly linked to human rights abuses through their investment in Novalpina Capital.[55]

Investors' human rights due diligence efforts can facilitate a broader understanding of investment risk and highlight the importance of access to transparent information on the operation of surveillance companies.

4. REVENUES RELIANT ON EXPLOITATION OF WIDELY USED DIGITAL PLATFORMS OFFERED BY MAJOR TECHNOLOGY COMPANIES

The business model of surveillance companies relies on the ongoing discovery and exploitation of vulnerabilities in widely used third-party digital platforms, such as Apple Inc's operating system, iOS, WhatsApp (owned by Facebook), Microsoft Windows, etc. Surveillance companies' profit thus partly depends on actively undermining the products of and ultimately generating costs to other technology manufacturers, with the end result that users of those platforms/operating systems are less secure. Consequently, investors in technology companies should also be concerned by the activities of the surveillance sector. Investors may also need to consider the risks of competing holdings if they are invested in both third-party platform companies and targeted surveillance companies.

For example, as part of the Pegasus Project, Amnesty International's forensic analysis uncovered irrefutable evidence that NSO Group's spyware successfully infected iPhone 11 and iPhone 12 models through exploiting vulnerabilities in iOS systems.[56] The threat of the private surveillance industry to other online platforms has led to a lawsuit, wherein WhatsApp and Facebook filed a case in California against NSO Group and Q Cyber Technologies alleging that the companies used WhatsApp servers to try and hack 1400 customer devices.[57] Technology giants such as Microsoft have participated in the WhatsApp lawsuit against NSO Group and supported calls for tougher regulation. In a statement entitled "Cyber mercenaries don't deserve immunity", a Microsoft corporate vice-president stated: "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."[58]

Investors in surveillance companies should assess the extent to which surveillance companies' activities are reliant on the exploitation of third-party platforms. They should also engage with relevant stakeholders to understand the risks posed by the private surveillance industry to privacy and security of third-party platforms.

5. LITIGATION RISK AGAINST PORTFOLIO COMPANIES

The techniques and operating methods of the digital surveillance industry regularly compromise the interests of third-party companies and consumers. In some cases, the surveillance activity might additionally amount to a violation of intellectual property law, consumer protection law, and contractual terms of service. This creates litigation risk and undermines consumer trust in and stability of third-party digital platforms. For example, as noted above, WhatsApp and Facebook filed a case in California against NSO Group and Q Cyber Technologies alleging that the companies used WhatsApp servers to try and hack 1400 customer devices.[59] This ongoing case has generated substantial participation from technology companies and civil society pushing back on NSO Group's novel arguments that it is entitled to immunity from legal action as it claims to be acting on behalf of its state agents. Those submitting briefs to the court included civil society groups and global technology companies such as Microsoft, Cisco, GitHub, Google, LinkedIn, VMWare, and the Internet Association on behalf of its members.[60]

At the time of writing this brief, and in response to the Pegasus Project, governments in Hungary[61], Belgium[62], and France[63] have launched investigations into the revelations. Victims of unlawful surveillance have initiated legal challenges in France[64] and India[65]. These judicial and governmental interventions are only expected to increase in the aftermath of the revelations.

Victims who have been unlawfully targeted with surveillance tools have brought legal challenges in other cases too. For instance, surveillance companies including Gamma Group[66], Amesys, and Qosmos have found themselves the subject of legal complaints[67]. As noted earlier, four executives of surveillance companies Amesys and Nexa Technologies were indicted by a Paris Court for complicity in torture over the sale of surveillance technology to governments in Libya and Egypt.[68] Previously, NSO Group's involvement in the unlawful targeted surveillance against human rights defenders and other civil society actors has also resulted in significant legal action against the company, including active litigation in Israel, Cyprus, the UK, and the USA.[69]

Additionally, petitioners in Israel brought an administrative action in 2019, supported by Amnesty International, to require the Israeli Ministry of Defence to revoke the export licence of NSO Group following the targeting of an Amnesty International staff member.[70] While the case was heard under a gag order[71] and the court ultimately declined to order revocation of the export licence,[72] it is an example of legal action to challenge the authorization of surveillance technology exports that may continue to emerge.

Litigation poses significant material risk to investors. Indeed, Moody's Investors Service has downgraded NSO Group's Corporate Family Rating citing "ongoing lawsuits", among a host of other reasons.[73]

6. LEGAL RISK DUE TO NON-COMPLIANCE WITH NEW REGULATION AND EVOLVING GOVERNMENT NORMS

The secrecy under which the surveillance industry operates together with revelations of its facilitation of human rights violations has led to increasing calls for a strong regulation over the industry. In 2019 the UN Special Rapporteur determined the problem was serious enough to warrant a "call not merely for tighter regulation of surveillance exports and restrictions on their use, but 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."[74]

The call for a moratorium is backed by a number of stakeholders including the UN High Commissioner for Human Rights[75], UN Special Procedures mandate holders[76], 150 civil society groups including Amnesty International, Access Now, Privacy International, Article 19, among many others[77], and companies such as Microsoft Corporation who urged leaders of tech firms to support an "immediate moratorium on the sale, transfer and use of dangerous spyware".[78]

Aside from a possible moratorium, relevant regulations in jurisdictions including the EU[79] and the USA are being strengthened. In the USA, it is likely that the Biden Administration will further build on moves made in 2020 when the Export Administration Regulations were revised to clarify that licensing decisions are based in part on "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."[80] For example, the Biden administration issued an executive order barring Americans from investing in Chinese firms linked to the country's military or engaged in selling surveillance that is used to repress dissent or religious minorities.[81]

In response to the Pegasus Project, authorities in Israel have set up a task force to look into revelations.[82] The European Commissioner for Justice has called for action on the issue of spyware.[83] New regulation and norms are only expected to evolve further.

7. QUESTIONS FOR INVESTORS TO ASK INVESTMENT MANAGERS AND SURVEILLANCE COMPANIES

QUESTIONS TO ASK INVESTMENT MANAGERS:

- Is the investor already exposed to the private surveillance industry via equity, fixed income, private equity and other investment vehicles? If so, what assessment has been undertaken by fund managers of the human rights and material risks arising from such investments and what mitigation strategy has been put in place to address them?
- Does your investment strategy allow for investment in companies selling targeted surveillance technologies?
- Is the investment manager required to notify the investor in advance of any new or additional investment in such companies?
- Do these companies provide specific details on their exports, including countries of export and end-user countries, to the investment manager?
- Are these companies subject to legal or contractual constraints limiting the information they can share with investors? If so, what are those limitations?

QUESTIONS TO ASK DIGITAL SURVEILLANCE COMPANIES

- Does the company conduct robust human rights due diligence and publicly disclose the steps taken to identify and assess, on an ongoing basis, human rights risks and develop mitigation measures for all proposed transactions before signing contracts? This should include consultations with affected stakeholders, including HRDs, civil society in destination countries and with relevant international NGOs.

- Does the company have publicly available human rights, whistleblowing, grievance and remedy policies, which include:
    - an adequate and transparent notification process for reporting misuse of technology and grievance mechanisms; and
    - robust mechanisms for compensation or other forms of redress for targets of unlawful surveillance?
- Has the policy been approved at the most senior levels of the company?
- Are such policies subject to regular audits by independent third-party observers to assess adequacy and compliance in their implementation, the results of which are publicly disclosed?
- Are company officials at the management level responsible for the monitoring of risks and overall implementation of this policy?
- What steps, if any, has the company's Board of Directors and/or executive leadership taken to understand the company's human rights risks and how it addresses or mitigates those risks?
- Does the company disclose regular information on sales/exports and contracts such as the type of product, volume, nature, value, destination and end-user countries?
- Does the company have a policy mandating it to refrain from exporting surveillance technology if there is a significant risk of human rights violations by end-user countries? Does the company track the implementation of this policy? Could the company provide examples of how this policy may have been applied citing concrete cases?
- Does the company implement contractual protections against human rights abuses including termination rights and confidentiality waivers in the case of misuse of its technology? Has the company terminated a contract due to misuse and if yes, how many times? Does the company track this information? Could the company provide examples?
- Does the company implement design and engineering choices that incorporate human rights protections? For example, by allowing for visibility over misuse of the technology or by providing checks on the number of client personnel who can operate the technology?
- Has the company faced or is the company facing any legal challenges, including from third-party technology companies, related to the sale or use of its technology? If the company has previously faced legal action, what was the outcome? What was the financial impact of the legal action?
- What would be the impact on their business of either a moratorium or increased integration of human rights issues into export controls?

8. CONCLUSION

Researchers, journalists, activists and others have for years documented significant evidence of the use of surveillance technology to target individuals around the world in violation of their internationally recognized human rights. The deployment of surveillance tools provided by private surveillance companies including NSO Group by government entities around the world, and the subsequent evidence of the use of such technologies against human rights defenders and civil society at large, exemplifies how readily these technologies can be used to undermine human rights. 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 investors. The questions in this briefing seek to help investors meet their own human rights responsibilities while mitigating investment risks as the legal, regulatory, and normative landscape continues to evolve.

ENDNOTES

[1] Report of the Special Rapporteur on Freedom of Opinion and Expression, May 2019, UN Doc. A/HCR/41/35, https://www.undocs.org/A/HRC/41/35

[2] Report of the Special Rapporteur on Freedom of Opinion and Expression, May 2019, UN Doc. A/HCR/41/35, https://www.undocs.org/A/HRC/41/35

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

[4] Amnesty International, "Uncovering the Iceberg, The Digital Surveillance Crisis Wrought by States and the Private Sector', 2021 https://www.amnesty.org/es/documents/doc10/4491/2021/en/

[5] Amnesty International and others, Operating from the Shadows: Inside NSO Group's Corporate Structure, May 2021. https://www.amnesty.org/en/documents/doc10/4182/2021/en/

[6] See: Privacy International, "Government Hacking" (Blog, date unknown), https://privacyinternational.org/learn/government-hacking

[7] 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/

[8] 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/

[9] See: Privacy International, "Government Hacking" (Blog, date unknown), https://privacyinternational.org/learn/government-hacking

[10] See Pegasus product description (leaked document), Page 40: Maintenance, Support and Upgrades https://www.documentcloud.org/documents/4599753-NSO-Pegasus.html#document/p23/a437977

[11] 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

[12] Amnesty International and others, Operating from the Shadows: Inside NSO Group's Corporate Structure, May 2020. https://www.amnesty.org/download/Documents/DOC1041822021ENGLISH.PDF

[13] Shulman, S, "Expect cyberattacks to up the ante says head of NSO Group", 12 April 2021, https://www.calcalistech.com/ctech/articles/0,7340,L-3904253,00.html

[14] Kleinman, M, "Pegasus spyware owner Novalpina to be liquidated after failure to resolve internal bust-up", 27 July 2021, https://news.sky.com/story/pegasus-spyware-owner-novalpina-to-be-liquidated-after-failure-to-resolve-internal-bust-up-12365638

[15] Kirchgaessner, S," US consultants lined up to run fund that owns Israeli spyware company NSO", 31 July 2021, https://www.theguardian.com/news/2021/jul/31/nso-group-israeli-spyware-company-berkeley-research-group

[16] NSO Group's Human Rights Policy. See: https://www.nsogroup.com/governance/human-rights-policy/

[17] Article 19, International Covenant on Civil and Political Rights.

[18] Article 17, International Covenant on Civil and Political Rights.

[19] UN Human Rights Committee General Comment 34, UN Doc. CCPR/C/GC/34, para. 23

[20] See: https://forbiddenstories.org/pegasus-project-articles/

[21] Amnesty International, "Uncovering the Iceberg, The Digital Surveillance Crisis Wrought by States and the Private Sector', 2021 https://www.amnesty.org/es/documents/doc10/4491/2021/en/

[22] See https://www.theguardian.com/world/2020/jan/16/israeli-spyware-firm-nso-hacking-case and https://www.theguardian.com/world/2020/feb/06/uk-to-host-spyware-firm-accused-of-aiding-human-rights-abuses

[23] R. Gallagher, "How Government-Grade Spy Tech Used A Fake Scandal To Dupe Journalists", *Slate*, 20 August 2012, https://slate.com/technology/2012/08/moroccan-website-mamfakinch-targeted-by-government-grade-spyware-from-hacking-team.html

[24] M. Marquis-Boire, "Backdoors are Forever: Hacking Team and the Targeting of Dissent?" *Citizen Lab*, 10 October 2012, https://citizenlab.ca/2012/10/backdoors-are-forever-hacking-team-and-the-targeting-of-dissent/

[25] M. Marquis-Boire & B. Marczak, "From Bahrain With Love: FinFisher's Spy Kit Exposed?", *Citizen Lab* 25 July 2012, https://citizenlab.ca/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/

[26]B. Marczak and others, "BAD TRAFFIC: Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?", *Citizen Lab*, 9 March 2018, https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/

[27] Electronic Frontier Foundation, "Kidane v. Ethiopia", date unknown https://www.eff.org/cases/kidane-v-ethiopia

[28] Amnesty International, "These Walls Have Ears: The Chilling Effect of Surveillance in South Sudan", 2021, https://www.amnesty.org/download/Documents/AFR6535772021ENGLISH.pdf

[29] International Federation of Human Rights, "Surveillance and torture in Egypt and Libya: Amesys and Nexa Technologies executives indicted" (Press Release, 22 June 2021) https://www.fidh.org/en/region/north-africa-middle-east/egypt/surveillance-and-torture-in-egypt-and-libya-amesys-and-nexa

[30] See for example: Novalpina Capital, Response to Open Letter to Novalpina Capital on 15 May 2019, www.amnesty.org/download/Documents/DOC10043620 19ENGLISH.PDF

[31] See https://www.amnesty.org/en/latest/research/2019/02/open-letter-to-novalpina-capital-nso-group-and-francisco-partners/, https://www.amnesty.org/en/latest/research/2019/04/second-open-letter-to-novalpina-capital-nso-group-francisco-partners/, https://www.novalpina.pe/response-to-open-letter-1/, and https://www.novalpina.pe/response-to-open-letter-2/

[32] Access Now et. al., "Rights Groups: NSO Group Continues to Fail in Human Rights" 27 April 2021, https://www.amnesty.org/en/documents/doc10/4036/2021/en

[33] See https://www.nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf

[34] Amnesty International, "NSO Group's new transparency report is "another missed opportunity"", June 2021 https://www.amnesty.org/en/latest/news/2021/07/nso-group-new-transparency-report-another-missed-opportunity/

[35] Amnesty International, "NSO Group's new transparency report is "another missed opportunity"", June 2021 https://www.amnesty.org/en/latest/news/2021/07/nso-group-new-transparency-report-another-missed-opportunity/

[36] See https://www.nsogroup.com/Newses/enough-is-enough/

[37] 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/

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

[39] Amnesty International and others, Operating from the Shadows: Inside NSO Group's Corporate Structure, May 2020. https://www.amnesty.org/download/Documents/DOC1041822021ENGLISH.PDF

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

[40] Defence Export Control Law 5766-2007 (Unofficial Translation), http://bitly.ws/dA72

[41] 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

[42] United Nations Human Rights Office of the High Commissioner, "Guiding Principles on Business and Human Rights", https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

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

[44] Amnesty International, Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group's Tools, June 2020 https://www.amnesty.org/en/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools/

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

[46] 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

[47] See: https://efile.fara.gov/docs/6170-Informational-Materials-20200618-467.pdf

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

[49] Amnesty International and others, Operating from the Shadows: Inside NSO Group's Corporate Structure, May 2020. https://www.amnesty.org/download/Documents/DOC1041822021ENGLISH.PDF

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

[51] United Nations Guiding Principles on Business and Human Rights, 2011, HR/PUB/11/04, Guiding Principles 11, and 13.

[52] United Nations Guiding Principles on Business and Human Rights, 2011, HR/PUB/11/04, Guiding Principles 15 and 17.

[53] 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

[54] 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.

[55] In October 2021, Amnesty International wrote to Alaska Permanent Fund Corps, Oregon Public Employees Retirement System, East Riding Pension Fund, and South Yorkshire Pensions Authority noting that they were directly linked to human rights abuse through their investment stake in Novalpina Capital, the private equity firm that backed the management buyout of NSO Group. This correspondence is available here. At the time of writing, Amnesty International did not receive a response from any of the funds except for the South Yorkshire Pensions Authority, who noted in an e-mail to Amnesty International on 12 October 2021 that it would not be making any further comment on these issues.

[56] Amnesty International, Pegasus Project: Apple iPhones compromised by NSO spyware, July 2021, https://www.amnesty.org/en/latest/news/2021/07/pegasus-project-apple-iphones-compromised-by-nso-spyware/

[57] See WhatsApp's lawsuit against NSO Group, https://www.washingtonpost.com/context/read-the-whatsapp-complaint-against-nso-group/abc0fb24-8090-447f-8493-1e05b2fc1156/

[58] 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/

[59] Kirchgaessner S, WhatsApp: Israeli firm 'deeply involved' in hacking our users, 29 April 2020 https://www.theguardian.com/world/2020/apr/29/whatsapp-israeli-firm-deeply-involved-in-hacking-our-users

[60] Microsoft Corp. and others, "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

[61] Boffey D, EU commissioner calls for urgent action against Pegasus spyware, September 2021, https://www.theguardian.com/news/2021/sep/15/eu-poised-to-tighten-privacy-laws-after-pegasus-spyware-scandal

[62] The Wire, Pegasus: Journalist, Wife Targeted by NSO Spyware, Finds Belgium's Military Intelligence, September 2021, https://thewire.in/tech/pegasus-journalist-wife-targetted-by-nso-spyware-finds-belgiums-military-intelligence

[63] Harwell, D and Birnbaum, M, France orders spyware investigation following Pegasus Project reports, July 2021, https://www.washingtonpost.com/world/2021/07/20/france-investigation-pegasus-spyware/

[64] Willsher, K, Pegasus spyware found on journalists' phones, French intelligence confirms, August 2021, https://www.theguardian.com/news/2021/aug/02/pegasus-spyware-found-on-journalists-phones-french-intelligence-confirms

[65] Mahapatra D, Supreme Court technical panel to probe Pegasus row, September 2021,

https://timesofindia.indiatimes.com/india/supreme-court-technical-panel-to-probe-pegasus-row/articleshow/86469187.cms

[66] European Center for Constitutional and Human Rights, German Prosecutor Opens Criminal Investigation into Finfisher for Selling Spyware to Turkey Without License, (Press Release), 5 September 2019, https://www.ecchr.eu/en/press-release/german-prosecutor-opens-criminal-investiation-into-finfisher-for-selling-spyware-to-turkey-without-license/

[67] 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

[68] International Federation of Human Rights, "Surveillance and torture in Egypt and Libya: Amesys and Nexa Technologies executives indicted" (Press Release, 22 June 2021) https://www.fidh.org/en/region/north-africa-middle-east/egypt/surveillance-and-torture-in-egypt-and-libya-amesys-and-nexa

[69] 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

[70] 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/

[71] 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/

[72] 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/

[73] See https://www.moodys.com/research/Moodys-downgrades-NSO-to-B3-with-negative-outlook--PR_446947

[74] Report of the Special Rapporteur on freedom of opinion and expression, UN Doc. A/HCR/41/35, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/76/PDF/G1914876.pdf?OpenElement

[75] Statement by United Nations High Commissioner for Human Rights, Michelle Bachelet at the Committee on Legal Affairs and Human Rights, Parliamentary assembly Council of Europe

Hearing on the implications of the Pegasus spyware, 14 September 2021
https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27455&LangID=E

[76] Spyware scandal: UN experts call for moratorium on sale of 'life threatening' surveillance tech, 12 August 2021, https://ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27379&LangID=E

[77] Amnesty International, et.al, Joint open letter by civil society organizations and independent experts calling on states to implement an immediate moratorium on the sale, transfer and use of surveillance technology, 27 July 2021 https://www.amnesty.org/en/documents/doc10/4516/2021/en/

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

[79] European Council of the European Union, "New rules on trade of dual-use items agreed", 9 November 2020 https://www.consilium.europa.eu/en/press/press-releases/2020/11/09/new-rules-on-trade-of-dual-use-items-agreed/

[80] Bureau of Industry and Security, Commerce, "Amendment to Licensing Policy for Items Controlled for Crime Control Reasons", 6 October 2020, https://www.bis.doc.gov/index.php/documents/regulations-docs/federal-register-notices/federal-register-2020/2638-85-fr-63007/file

[81] The New York Times, Biden Expands Trump-Era Ban on Investment in Chinese Firms Linked to Military, June 2021 https://www.nytimes.com/live/2021/06/03/us/biden-news-today#biden-china-surveillance-order

[82] Williams, D, Israel appoints task force to assess NSO spyware allegations -sources, July 2021, https://www.reuters.com/technology/israels-national-security-council-looking-into-nso-spyware-allegations-2021-07-21/

[83] Boffey, D, EU commissioner calls for urgent action against Pegasus spyware, September 2021, https://www.theguardian.com/news/2021/sep/15/eu-poised-to-tighten-privacy-laws-after-pegasus-spyware-scandal

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 IN THE SHADOWS

INVESTOR RISK FROM THE PRIVATE SURVEILLANCE INDUSTRY

Many states enhance their surveillance capabilities by buying spyware or other digital surveillance tools from surveillance companies. While governments claim to use these to fight crime and terrorism, many have used them to target human rights defenders, activists, journalists and members of civil society in violation of their internationally recognized human rights. This is done by attempting to, and in many cases successfully compromising their digital devices to monitor their activities and communications and obtain access to their private data. Such targeted digital surveillance is ultimately used to harass, intimidate, and persecute those targeted.

Given the scale of disclosures revealed in the Pegasus Project, there is an urgent need for investors to assess risk of investments in the private surveillance industry. This briefing outlines the material risks, including reputational, financial, and legal risks facing companies and investors in this sector. It uses the surveillance company NSO Group as a case study, as the company and its functioning exemplify the risk that the poorly regulated surveillance industry poses. We suggest questions for investors and potential investors to ask investment managers and surveillance companies in order to understand whether these risks and impacts are being adequately assessed, prevented, mitigated and managed.

INDEX: DOC 10/4359/2021
MONTH/YEAR: OCTOBER 2021
LANGUAGE: ENGLISH

amnesty.org

AMNESTY INTERNATIONAL