UNCOVERING THE ICEBERG

THE DIGITAL SURVEILLANCE CRISIS WROUGHT BY STATES AND THE PRIVATE SECTOR

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 10/4491/2021
Original language: English

amnesty.org

Cover illustration: *© Toscanabanana 2021*

AMNESTY INTERNATIONAL

CONTENTS

1. INTRODUCTION

At the launch of a platform[1] designed to track the deployment and human rights impacts of the targeted digital surveillance tools of NSO Group (developed by Forensic Architecture with the support of Amnesty International and the Citizen Lab), whistle-blower Edward Snowden spoke. He commented: "I think the investigation of not just the NSO Group, but this sector and this technology, is the most important unwritten story in media today."[2] Indeed, civil society has long reflected that the pervasive lack of transparency around the use of targeted digital surveillance, and the role of the private sector in facilitating that surveillance, has impeded understanding of and accountability for the severe human rights repercussions of the trade. We cautioned that the few, hard-won insights that civil society, journalists, and researchers were able to obtain – regarding NSO Group and a handful of other surveillance companies such as Hacking Team and FinFisher – were just the tip of the iceberg.

Now, as a result of collaborative investigation that involves more than 80 journalists from 17 media organizations in 10 countries coordinated by Forbidden Stories with technical support from Amnesty International, Snowden-scale disclosures have 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 physical safety. The investigation reveals that Human Rights Defenders, journalists, lawyers, activists and politicians across the globe have been potentially targeted in this nearly global assault on privacy.

As part of the investigation, Technologists at Amnesty Tech's Security Lab were able to identify traces of NSO's "zero-click" attacks (malware infections that require no interaction with the target) through cutting edge forensic analysis, including by linking these new attacks to previously documented attacks on human rights defenders (HRDs) using NSO Group software.[3] This project was a crucial and overdue breakthrough of transparency in an industry stubbornly resistant to it, which relied on the collaborative efforts of all involved. It is important to note, however, that the success of such investigative efforts was never guaranteed, and these disclosures cannot represent the only form of check on industry participants and state actors.

The stories published as a result of this collaboration speak for themselves. In this briefing, Amnesty International's goal is to contribute to the discussion by highlighting some of the key insights from the perspective of international law, particularly international human rights law, that come out of the reporting and technical analyses. These include: the improper breadth of targeting under international human rights law, which is also out of line with the company's stated rationale of selling its products to help its clients combat crime, including terrorism-related conduct; the clandestine nature of the tool that facilitates its illegal use and operation; the serious human rights violations that have resulted; the total impunity of states and companies in deploying this targeted digital surveillance tool; and the failure of states to fulfil their obligation to protect them from this unlawful hacking and surveillance.

---

[1] Forensic Architecture, Amnesty International and Citizen Lab, *Digital Violence*, digitalviolence.org.

[2] Aaron Schaffer, The Cybersecurity 202: Group maps alleged victims of NSO Group surveillance tool, *The Washington* Post, 6 July 2021, washingtonpost.com/politics/2021/07/06/cybersecurity-202-group-maps-alleged-victims-nso-group-surveillance-tool.

[3] Amnesty International, *Forensic Methodology Report: How to Catch NSO Group's Pegasus*, 18 July 2021, amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus.

Finally, Amnesty International puts forward recommendations on the way forward, given the demonstrated need for independent oversight of the targeted digital surveillance industry, accountability for human rights violations and abuses, and greater transparency. For if these revelations are what we can expect in connection from a company that claims to respect human rights in line with the UN Guiding Principles on Business and Human Rights (UN Guiding Principles),[4] what hope is there with respect to the wide range of surveillance activity made possible by the surveillance industry at large? The revelations lead to one conclusion: This is an unaccountable industry, and an unaccountable sphere of state practice, that must not continue to operate in their current forms. Our human rights and the security of the digital ecosystem as a whole depend on it.

For years Amnesty International has warned of the human rights dangers posed by unlawful surveillance generally[5] and the targeted surveillance industry and NSO specifically[6]. These revelations shed new light on the urgent need for meaningful control over the rampant abuses we now conclusively know are being carried out. These disclosures make clear that when states fail to respect human rights through surveillance, or fail in their duties to protect us against human rights abuses by companies at home or abroad, these same companies will be able to continue flouting their human rights responsibilities with impunity.

[4] NSO Group, *Transparency and Responsibility Report 2021*, 30 June 2021, nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf.

[5] Amnesty International, *"It's Enough for People to Feel It Exists": Civil Society, Secrecy and Surveillance in Belarus*, (Index: EUR 49/4306/2016), 7 July 2016, amnesty.org/download/Documents/EUR4943062016ENGLISH.PDF; Amnesty International, "We Will Find You, Anywhere": The Global Shadow of Uzbekistani Surveillance, *Medium*, 30 March 2017, medium.com/amnesty-insights/we-will-find-you-anywhere-the-global-shadow-of-uzbekistani-surveillance-254405805860, Amnesty International, "UK, Europe's Top Court Rules UK Mass Surveillance Regime Violated Human Rights", 25 May 2021, amnesty.org/en/latest/news/2021/05/uk-surveillance-gchq-ecthr-ruling.

[6] 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), 20 December 2019, amnesty.org/download/Documents/ACT3013852019ENGLISH.PDF; Amnesty International, *Pakistan: Human Rights under Surveillance*, (Index: ASA 33/8366/2018), 15 May 2018, amnesty.org/en/documents/asa33/8366/2018/en; Amnesty International, *Moroccan Journalist Targeted with Network Injection Attacks Using NSO Group's Tools*, 22 June 2020, amnesty.org/en/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools.

2. INSIGHTS REGARDING INTERNATIONAL HUMAN RIGHTS LAW AND THE PEGASUS PROJECT REVELATIONS

2.1 IMPROPER BREADTH OF TARGETING WITH SERIOUS HUMAN RIGHTS CONSEQUENCES

It is the legal obligation of states to protect against the sorts of abuses revealed to have been carried out by private companies such as NSO Group. However, these revelations confirm what we have long known – that many states have little interest in respecting, let alone protecting human rights, when it comes to surveillance. The failure of states to put a meaningful check on NSO Group has led to human rights abuses on a grand scale.

THE RESPECTIVE HUMAN RIGHTS OBLIGATIONS OF STATES AND COMPANIES

Nation states have binding obligations under international human rights law to protect human rights from abuse by third parties.[7] This includes the obligation to regulate the conduct of companies who are domiciled there or are under their effective control in order to prevent them from causing or contributing to human rights abuses even if they occur in other countries.[8]

As laid out in the UN Guiding Principles on Business and Human Rights (UNGPs), companies also have a responsibility to respect human rights wherever they operate in the world. The UNGPs require that companies take proactive steps to ensure that they do not cause or contribute to human rights abuses within their global operations, and to respond to any human rights abuses when they do occur. In order to meet that responsibility, companies must carry out human rights due diligence to "identify, prevent, mitigate and account for how they address their human rights impacts." The corporate responsibility to respect human rights exists independently of a state's ability or willingness to fulfil its own human rights obligations and over and above compliance with national laws and regulations protecting human rights. For example, the interpretative guidance on the UNGPs specifically notes that a company may contribute to a human rights violation if it provides "data about Internet service users to a Government that uses the data to trace and prosecute political dissidents contrary to human rights".[9]

Moreover, it is possible that a company that sells surveillance equipment could be complicit in any subsequent violation of human rights in which the equipment it supplies is used. An International Commission of Jurists (ICJ) Panel of Experts has examined the question of corporate complicity in human rights violations in some depth and clarified how legal liability, both civil and criminal, could arise for such complicity. The ICJ panel considered that there could be a sufficiently close link in law if the company's conduct enabled, exacerbated or facilitated the abuse, and the company knew, or ought reasonably to have known, that the abuse would occur. A company could enable, exacerbate or facilitate abuse through, among other things, the provision of goods or services.[10]

NSO Group has often asserted, as the rationale for its existence (and its opacity) that the "sole purpose of NSO is to provide technology to licensed government intelligence and law enforcement agencies to help them fight terrorism and serious crime."[11] The company has relied on the premise that the tool is legitimately used for and essential to countering terror and catching criminals in order to rally public and official support for its unfettered operations.

The Pegasus Project disclosures blow that premise wide open.

---

[7] UN Human Rights Committee (HRC), General Comment 31 [80]: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, UN Doc. CCPR/C/21/Rev.1/Add. 13, para. 8.

[8] States are responsible for protecting against abuses by private companies even outside of their borders. This principle is well-accepted and directly applicable to rights infringed in the cases revealed in this project. See, e.g. UN Committee on Economic, Social and Cultural Rights (CESCR), General Comment 14: State obligations under the International Covenant on Economic, Social and Cultural Rights in the context of business activities, 10 August 2017, UN Doc. E/C.12/GC/24, § III.C.2.; UN Human Rights Committee (HRC), General Comment 36: Right to Life, 3 September 2019, UN Doc. CCPR/C/GC/36, para. 63; see also UN Special Rapporteur on extrajudicial, summary or arbitrary executions, Annex to the Report: *Investigation into the unlawful death of Mr. Jamal Khashoggi*, 19 June 2019, UN Doc. A/HRC/41/CRP.1.

[9] United Nations Office of the High Commissioner for Human Rights, *The Corporate Responsibility to Respect Human Rights: An Interpretive Guide*, ohchr.org/Documents/Publications/HR.PUB.12.2_En.pdf, p. 17.

[10] International Commission of Jurists (ICJ), *Report of the ICJ Expert Legal Panel on Corporate Complicity in International Crimes*, 1 January 2008, icj.org/report-of-the-international-commission-of-jurists-expert-legal-panel-on-corporate-complicity-in-international-crimes.

[11] NSO Group, "NSO Group Statement on Facebook Lawsuit", *CISION PR Newswire*, 30 October 2019, prnewswire.com/il/news-releases/nso-group-statement-on-facebook-lawsuit-832166037.html. See also NSO Group, *Transparency and Responsibility Report 2021*, 30 June 2021, nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf, excerpt of Contract Provisions at p. 31: "The end user hereby represents and warrants that it and its respective employees and agents: . . . (iii) shall use the System only for the legitimate and lawful prevention and investigation of serious crimes and terrorism, as defined in Exhibit F or in domestic law in a manner substantially similar to Exhibit F, with the definitions in Exhibit F controlling in cases of any material conflict between the definition of such crimes in domestic law and Exhibit F[.]".

As reported for years, while this tool may be marketed for legitimate purposes – to "collect data from the mobile devices of specific suspected major criminals"[12] – there is a simultaneous parallel use of the tool against civil society and other people in violation of international human rights law. The window of insight obtained through this collaborative investigation confirms just how enormous in scale that parallel use is, as well as the potentially destabilizing impact of the tool on not only human rights, but also the security of the digital environment at large.

The scope of the unlawful targeting with NSO Group's tools revealed in this project span the world, and reveal potential targets that include world leaders, politicians, human rights defenders (HRDs), and journalists. 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 brazen targeting of the family, friends and associates of murdered journalist Jamal Khashoggi demonstrate not only the disdain for the targets' human rights, but the evident impunity with which states deploy this tool. According to reporting, Khashoggi's wife, Hanan Elatr, was targeted with Pegasus spyware four months prior to Khashoggi's murder.[13] In the days immediately following his killing, the phone of his fiancée, Hatice Cengiz, was successfully infected with Pegasus multiple times. Another associate of Khashoggi's – the former Al Jazeera journalist Wadah Khanfar – was also successfully infected with Pegasus.[14]

This case is emblematic of so many of the harms caused by the use of this NSO Group tool. It allows spying not only on unlawful targets such as journalists, but can easily be extended to their associates, families or networks, with devastating real-world effects that reach far beyond the harms to the targets' privacy. As The Washington Post notes in their investigation of these attacks: "The disruption in the lives of the two women in Khashoggi's life shows the impact that even the fear of spying can have. Both of them had fulfilling, independent lives before they began a romantic relationship with him; both now live in hiding and have been forsaken by friends who fear for their own safety because they know authorities can link them via their phones and through social media, texts and other communications."[15]

While it is impossible to ascertain the full scope of targeting enabled by this tool, the information that has emerged thus far clearly indicates that its unspoken parallel use – to engage in surveillance that violates human rights, endangers individuals is far more significant than the company anti-crime, anti-terrorism narrative lets on. This set of persons of interest, targets and victims may in fact constitute a sizeable percentage of the total licences issued to the company by the Israeli Ministry of Defence (only an independent audit of the Pegasus spyware licences issued to NSO Group could verify the figures with certainty). And as discussed throughout the stories and in more depth below, the company either knew or should have known of such pervasive and improper end use.[16]

These stories also illustrate the disturbing link between targeted digital surveillance, privacy abuses and other human rights abuses. In terms of operational capacity, this surveillance tool has no limits: every piece of data that traverses an infected device is accessible, while the tool covers its tracks and is designed to

---

[12] NSO Group, *Transparency and Responsibility Report 2021*, 30 June 2021, nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf, p. 7.

[13] Because Elatr was using an Android phone, Amnesty technologists were not able to confirm whether the targeting of Elatr was successful.

[14] Dana Priest, Souad Mekhennet and Arthur Bouvart, "Jamal Khashoggi's wife targeted with spyware before his death," *The Washington Post*, 18 July 2021, washingtonpost.com/investigations/interactive/2021/jamal-khashoggi-wife-fiancee-cellphone-hack.

[15] Dana Priest, Souad Mekhennet and Arthur Bouvart, "Jamal Khashoggi's wife targeted with spyware before his death," *The Washington Post*, 18 July 2021, washingtonpost.com/investigations/interactive/2021/jamal-khashoggi-wife-fiancee-cellphone-hack.

[16] An International Commission of Jurists (ICJ) Panel of Experts has examined the question of corporate complicity in human rights violations in some depth and clarified how legal liability, both civil and criminal, could arise for such complicity. The ICJ panel considered that there could be a sufficiently close link in law if the company's conduct enabled, exacerbated or facilitated the abuse, and the company knew, or ought reasonably to have known, that the abuse would occur. A company could enable, exacerbate or facilitate abuse through, among other things, the provision of goods or services. International Commission of Jurists (ICJ), *Report of the ICJ Expert Legal Panel on Corporate Complicity in International Crimes*, 1 January 2008, icj.org/report-of-the-international-commission-of-jurists-expert-legal-panel-on-corporate-complicity-in-international-crimes.

avoid leaving or destroy any evidence of its use. Given the targets, history, and context, one can conclude that individuals' most sensitive data – physical location, surreptitiously recorded video content, individual contacts, photos, private chats, personal medical details – has been marshalled and turned against them, without any subsequent notification, or opportunity to challenge the surveillance. The outcomes of such targeting are potentially disastrous, particularly with respect to interception of intimate personal data and its use as emotional leverage.

Additionally, the scale and breadth of the targeting may in fact reveal only part of the picture of human rights harms that they signify. This is true for several reasons. One is that – as these stories dramatically illustrate – unlawful surveillance may impact on people beyond the target themselves, including family, friends, colleagues and others. As the Hungarian journalist András Szabó reflected upon being notified that his phone had been targeted with Pegasus software: "I started thinking about what these hackers were able to find out about me through my phone's data. Were they searching for my sources? Did any of them get into trouble?".[17] Azerbaijani investigative journalist Khadija Ismayilova reacted similarly to learning of her phone's infection, as recounted by the Organized Crime and Corruption Reporting Project (OCCRP):

> **"in the immediate moment, the main concern was whether she had compromised anyone else. She thought about it all night, trying to remember what she had sent and to whom.**
>
> **'It's devastating,' she said the next day. 'You make everyone a target.'**
>
> **As she scrolled through the list of more than 1,000 Azerbaijani numbers in the leak, she recognized number after number: A niece. A friend. Her taxi driver.**
>
> **'Him too,' she cried again and again. 'Her too.'"[18]**

This is also true because violations of the right to privacy impact on numerous other human rights. For example, the UN High Commissioner for Human Rights has noted that "[t]echnology-enabled surveillance poses significant risks to the enjoyment of human rights in peaceful assemblies and is an important contributor to the shrinking of civic space in many countries."[19] The same is true of the right to freedom of expression, association and other human rights, and may have unforeseen harms on specific groups, especially those who face discrimination based on their identity or identities.

Moreover, where surveillance is operated without adequate oversight, safeguards and transparency, the harms of unlawful surveillance impact far beyond those who may have actually been targeted. It is well known that "even the possibility of communications being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association."[20] In the face of opacity and inadequate safeguards, and especially in situations where surveillance is known or suspected to be carried out in unlawful ways, human rights defenders are forced to self-censor out of fear of being criminalized for their work, even where such surveillance may in fact not be taking place. Numerous research reports by Amnesty International reveal how this chilling effect can have a serious and detrimental effect on global civil society. As one Belarusian HRD noted regarding the impact of secret surveillance on their work, "[i]t's enough for people to feel it exists."[21]

---

[17] Organized Crime and Corruption Reporting Project (OCCRP), *András Szabó: Hungarian Journalist*, 18 July 2021, occrp.org/en/the-pegasus-project/andras-szabo-hungarian-journalist.

[18] Miranda Patrucic and Kelly Bloss, "Life in Azerbaijan's Digital Autocracy, 'They Want to be in Control of Everything'", *OCCRP*,18 July 2021, occrp.org/en/the-pegasus-project/life-in-azerbaijans-digital-autocracy-they-want-to-be-in-control-of-everything.

[19] UN High Commissioner for Human Rights, Report: *Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests*, 24 June 2020, UN Doc. A/HRC/44/24, para. 24.

[20] UN Office of the High Commissioner for Human Rights (OHCHR), Report: *The Right to Privacy in the Digital Age*, 30 June 2014, UN Doc. A/HRC/27/37, para. 20.

[21] Amnesty International, *"It's Enough for People to Feel It Exists": Civil Society, Secrecy and Surveillance in Belarus*, (Index: EUR 49/4306/2016), 7 July 2016, amnesty.org/download/Documents/EUR4943062016ENGLISH.PDF.

By allowing NSO Group software to be used unchecked, without taking adequate steps to protect our rights, states have allowed a scandal to flourish that has touched on the rights of many people all over world, in more ways, than we may ever be able to catalogue.

2.2 SEVERE INTRUSION, MINIMAL SAFEGUARDS

The Pegasus Project disclosures paint a picture of a company and targeted digital surveillance methods that have slipped through the – admittedly large – cracks of existing legal and regulatory systems at domestic, regional, and international levels. Pegasus software is designed to be an extraordinarily severe interference with the right to privacy. Despite this, very few safeguards from states or the company itself exist that could render the interferences demonstrated in these revelations proportionate, and thus lawful. NSO Group's targeted digital surveillance tool is designed and employed in ways that make the violations we have seen sadly predictable.

Importantly, it must be recognized that there is no use of a targeted digital surveillance tool such as Pegasus that does not implicate the internationally recognized right to privacy, and by implication, often many other rights.[22] The use of Pegasus spyware impacts the right to privacy by design: it is surreptitious, unauthorized by the rights holder, and has the capacity to collect and deliver an unlimited selection of personal and private data (along with data of any contacts with which a target of surveillance interacts).

Technical measures exist that could provide some checks on this invasive tool, but there is no evidence that NSO Group employ these. In their *Transparency and Responsibility Report*, for instance, they note:

> **"[Human rights] concerns are heightened because we are unable to monitor immediate use, and have not yet determined whether there could be a technological solution to prevent customers from targeting vulnerable populations. We compensate through robust contractual terms that seek to institute processes aligned with international standards, and an enhanced review process aimed at screening out customers where the rule of law is weak, local laws do not meet international norms, or customers are unable or unwilling to provide sufficient assurances."[23]**

Relying on contractual promises from states determined to have weak track records of adherence to their other legal obligations, including international human rights legal obligations, is an evidently weak check on abuse.

Moreover, rather than proactively investigating abuses, NSO Group – by their own account – wait until notified to initiate investigations. Despite claims to have discontinued or foregone several contracts over the last few years, the difficulty in identifying cases of abuse of such a secretive tool, coupled with the lack of remedies or safeguards for victims, also make this an ineffective safeguard, contrary to best practices.

Moreover, as noted above, a violation of the right to privacy can have cascading effects on other rights. The question, therefore, is whether the particular application of this tool constitutes a permissible interference with the right to privacy.[24] As will be demonstrated, it is evident from these disclosures that it does not.

---

[22] Court of Justice of the European Union, Case No. C-111/18 ("Schrems II"), 16 July 2020, para. 171: "The Court has held that the communication of personal data to a third party, such as a public authority, constitutes an interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, whatever the subsequent use of the information communicated". See also European Court of Human Rights, *Szabo* §53, *Zakharov §179, Klass* §41.

[23] NSO Group, *Transparency and Responsibility Report 2021*, 30 June 2021, nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf, pp. 18-19.

[24] "A limitation can only be lawful and non-arbitrary if it serves a legitimate purpose" (see UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report: *Use of encryption and anonymity in digital communications*, 22 May 2015, UN Doc. A/HRC/29/32, para. 33).

"The limitation must be necessary for reaching that legitimate aim and in proportion to that aim and must be the least intrusive option available. Furthermore, any limitation to the right to privacy must not render the essence of the right meaningless" (see UN Secretary-General (UNSG), Note: *Promotion and protection of human rights and fundamental freedoms while countering terrorism*, 23 September 2014, UN Doc. A/69/397, para. 51). UN United Nations High Commissioner for Human Rights, Report: *The right to privacy in the digital age*, 3 August 2018, UN Doc. A/HRC/39/29, para. 10.

International human rights law requires that every deployment of this tool meet the test to establish a permissible restriction of a guaranteed right: the deployment must comply with the principles of legality, necessity and proportionality, and must serve a legitimate purpose. In other words, the mere assertion of a potentially legitimate interest is not enough to justify restrictions on the right to privacy, unless the other requirements of human rights law are met. The well accepted legal fact is reflected in, inter alia, the UN Global Counter-Terrorism Strategy, which recognizes that "[m]easures to ensure respect for human rights for all and the rule of law as the fundamental basis for the fight against terrorism" as one of its four pillars. It reaffirms "that States must ensure that any measures taken to combat terrorism comply with their obligations under international law, in particular human rights law, refugee law and international humanitarian law."[25] Further, the most recent review of the Strategy, "[c]alls upon States, while countering terrorism and preventing violent extremism conducive to terrorism, to review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy, as set out in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights, by ensuring the full and effective implementation of all their obligations under international human rights law."[26]

In practice, however, no adequate overarching framework exists to ensure fulfilment of these requirements when it comes to targeted digital surveillance operations.[27] Indeed, many states have sought to preserve a wide latitude of operation domestically and extraterritorially, and secrecy regarding the targeted digital surveillance tools at their disposal. States have relied on export regulation as the primary means of control of deployment of this tool, but that approach has, predictably, failed to curb human rights violations. Export licensing decisions are made at the discretion of the state, and do not incorporate objective disqualifying criteria (aside from the sanctions regimes that apply against a handful of states), thus leaving the door open to state approval based on competing priorities, and preserving state flexibility in this area.[28] While some states, and notably also the European Union (EU), have attempted to impose human rights criteria on surveillance exports, this has also failed to provide a meaningful check. The EU, for example, despite civil society calls, adopted its final dual-use export regulation[29] that requires only that states "consider" human rights criteria as part of their assessment when granting export licences, but leaves them free to grant them all the same. Such loopholes in the regulation give states free reign to ignore the human rights risks related to the export of these tools. Although theoretically other EU law should also require the consideration of human rights in exports, it is clear from the record of EU technology being used to repress rights that this is ineffective in practice.[30]

Moreover, by subsuming a purported "lawful intercept" tool such as Pegasus within historically unaccountable state intelligence operations writ large, states have blurred the boundaries of permissible use of the tool, at the expense of the principles of legality, necessity, proportionality and legitimate aim. NSO Group itself has acknowledged that its tool may serve unlawful ends and contribute to adverse human rights

---

[25] UN General Assembly (UNGA) Resolution 16/288: The United Nations Global Counter-Terrorism Strategy, adopted on 8 September 2006, UN Doc. A/RES/60/288.

[26] UN General Assembly (UNGA) Resolution 72/284: The United Nations Global Counter-Terrorism Strategy Review, adopted on 26 June 2018, UN Doc. A/RES/72/284, para. 20.

[27] As the UN Special Rapporteur on Freedom of Opinion and Expression has noted: "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." UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report: *Surveillance and Human Rights*, 28 May 2019, UN Doc. A/HRC/41/35, para. 46.

[28] Access Now and others, *Human Rights Organizations' Response to the Adoption of the New EU Dual Use Export Control Rules*, March 2021, hrw.org/sites/default/files/media_2021/03/Reforms%20to%20EU%20Surveillance%20Tech%20Export%20Rules_Joint%20NGO%20Statement_20210324_0.pdf.

[29] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast), eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2021:206:FULL&from=EN.

[30] Amnesty International, *Out of Control: Failing EU Laws for Digital Surveillance Export*, (Index: EUR 01/2556/2020), 21 September 2020, amnesty.org/en/documents/EUR01/2556/2020/en.

impacts.[31] However, the company has maintained the position that it may continue to supply its clients without actually verifying end use – even in the face of numerous instances of documented abuses – due to allegedly overriding national security interests.[32]

The mere assertion of national security, without the required demonstration of legality, necessity, proportionality or legitimate aim,[33] has sufficed to justify the continued supply and operation of the tool. Notably, while the company has regularly invoked counterterrorism requirements as part of this rationale, it has never explained how the design or use of its tool aligns with the substantial body of legal, policy and body of work developed in recent years concerning promotion and protection of human rights while countering terrorism (e.g., the UN Global Counter-Terrorism Strategy,[34] and the extensive work of the UN Special Rapporteur on counterterrorism and human rights, including on topics such as best practices for intelligence services[35]). NSO Group's June 2021 *Transparency and Responsibility Report* instead incongruously asserted an "absence of best practices and guidance both for states and our industry to appropriately balance human rights and individual liberties with the demands of the fight against major crimes and terrorism"[36] – summarily dispensing with decades of relevant efforts and legal human rights standards. NSO Group's assertion is incorrect, as the UN Special Rapporteur on Freedom of Opinion and Expression has called on the surveillance industry generally and written to NSO Group specifically to urge the adoption of international human rights-compliant standards in their work, including, inter alia, the use of technical limitations to reduce the potential for human rights harms.[37]

NSO Group, Israel (as the state in which NSO Group is primarily based), and the states described in these stories that have deployed the tool against a sweeping array of targets, are thus prioritizing the restriction before the right in providing and/or operating this targeted digital surveillance tool. Yet, as the UN High Commissioner for Human Rights has emphasized, "any limitation to the right to privacy must not render the essence of the right meaningless."[38] In the wake of such reversal, targeted digital surveillance has grown into

---

[31] NSO Group, *Transparency and Responsibility Report 2021*, 30 June 2021, nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf, pp. 9; 17-19.

[32] See, e.g., NSO Group, *Transparency and Responsibility Report 2021*, 30 June 2021, nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf, pp. 9-10 ("Our customers are solely authorized intelligence and law enforcement agencies responsible for investigating and, where possible, preventing serious crimes and terrorist acts. To effectively conduct these types of operations, these agencies must operate discreetly in order to (i) infiltrate criminal and terrorist networks to obtain information critical to stopping illegal acts, and (ii) avoid inadvertently giving criminals and terrorists a chance to thwart preventive activities. As a result, our customers mandate strict confidentiality from us and all other service providers in our sector. Our capacity for action is also limited by the fact that we do not have visibility into the specific operational uses of our products, unless that access is granted by the customer (as contractually required in the event of an investigation of suspicion that the system has been misused). Nonetheless, this report provides insights into how we operationalize our mission, and contribute to balance the tensions between the duties of states to protect their populations from physical and criminal threats with their obligations towards freedom of expression, the right to privacy and other human rights.").

[33] Neither the company nor state export authorities have described verification of end-user fulfilment of these requirements as part of company due diligence or mitigation mechanisms, or export licence decisions.

[34] The UN Global Counter-Terrorism Strategy recognizes as one of its four pillars: "Measures to ensure respect for human rights for all and the rule of law as the fundamental basis for the fight against terrorism." It reaffirms "that States must ensure that any measures taken to combat terrorism comply with their obligations under international law, in particular human rights law, refugee law and international humanitarian law." UN General Assembly (UNGA) Resolution 16/288: The United Nations Global Counter-Terrorism Strategy, adopted on 8 September 2006, UN Doc. A/RES/60/288.

[35] UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, Report: *Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight*, 17 May 2010, UN Doc. A/HRC/14/46.

[36] NSO Group, *Transparency and Responsibility Report 2021*, 30 June 2021, nsogroup.com/wp-content/uploads/2021/06/ReportBooklet.pdf, p. 30. Moreover, the notion of "balancing" between human rights and security is itself misplaced. As the UN Special Rapporteur on counterterrorism and human rights has explained, ""effective counterterrorism measures and the protection of human rights are not conflicting, but rather complementary and mutually reinforcing goals. This also reflects the flexibility of human rights law. Through the careful application of human rights law it is possible to respond effectively to the challenges involved in the countering of terrorism while complying with human rights. There is no need in this process for a balancing between human rights and security, as the proper balance can and must be found within human rights law itself. Law is the balance, not a weight to be measured." UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, Report: *Ten areas of best practices in countering terrorism*, 22 December 2010, UN Doc. A/HRC/16/51, para 12.

[37] Letter from UN Special Rapporteur for Freedom of Expression, David Kaye, to Shalev Hulio, NSO Group, 18 October 2019, spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=24905.

[38] UN Human Rights Committee (HRC), General Comments Adopted by the Human Rights Committee under Article 40, Paragraph 4, of the International Covenant on Civil and Political Rights No. 27: Article 12 (Freedom of Movement), 1 November 1999, UN Doc. CCPR/C/21/Rev.1/Add.9, para 13.

a widespread practice and supporting industry that effectively evade any accountability on the basis of existing legal and regulatory regimes.

For example, the targeted digital surveillance tools provided by NSO Group are nowadays constructed around vulnerabilities in consumer-facing digital applications and platforms. States have effectively incentivized private sector actors to seek out vulnerabilities in popular digital devices and applications, and determine methods of utilizing them for offensive purposes rather than engaging in responsible disclosure – thus raising the bar on surveillance capabilities, undermining other technology providers, and compromising the security of the digital environment for users across the globe. While surveillance companies generate revenue from this activity, affected third-party providers (many of which are publicly traded companies) must allocate significant resources to address discovered breaches in order to ensure user security and retention. Pegasus is able to bypass security safeguards on new models of Apple iPhones, potentially undermining the security of all iPhone users. Moreover, by delivering malware via "zero-click" attacks (malware infections that require no interaction with the user in order to install themselves), NSO Group has created a tool that creates a devastating impact on privacy, while at the same time requiring very little effort from governments who wish to target people broadly for unlawful surveillance.[39]

When asked what people can do to protect themselves from Pegasus, the whistle-blower Edward Snowden commented: "[w]hat can people do to protect themselves from nuclear weapons?".[40] Indeed, there is nothing an individual user can meaningfully do to protect oneself from a Pegasus "zero-click" attack. The only true protection lies in collective protection through robust law and regulation, but, as has been revealed clearly by this investigation, what law there is has failed. This failure has come back to haunt states themselves in a dramatic illustration of the tool's extraterritorial impact and potential to affect rights even in other states. According to The Washington Post's investigation, hundreds of politicians, including 14 heads of state, were potential targets for infection.[41] International dialogue around cyber norms and application of international law to state cyber operations has been underway for many years.[42] Norms concerning digital espionage during peacetime, however, have not yet fully crystallized. However, from these revelations, it is clear that states are undertaking the targeting of individuals for the exercise of their internationally recognized human rights, interfering with the ability of other states to conduct their own affairs and meet their own human rights obligations.[43]

2.3 STATE WRONGS AND CORPORATE COMPLICITY

These revelations – with research stretching over years, demonstration of serious rights impacts, a clear lack of compliance with international law and standards, yet no actual repercussions to or changes in activity by the company or its clients – lead to the conclusion that **states and companies engage in targeted digital surveillance with impunity**.

A culture of impunity specific to targeted digital surveillance has developed in the absence of adequate law and oversight. As the former UN Special Rapporteur on Freedom of Opinion and Expression has noted: "[d]igital surveillance is no longer the preserve of countries that enjoy the resources to conduct mass and targeted surveillance based on in-house tools. Private industry has stepped in, unsupervised and with

---

[39] Amnesty International, "Pegasus Project: Apple iPhones compromised by NSO spyware", 19 July 2021, amnesty.org/en/latest/news/2021/07/pegasus-project-apple-iphones-compromised-by-nso-spyware.

[40] David Pegg and Paul Lewis, "Edward Snowden calls for spyware trade ban amid Pegasus revelations", *The Guardian*, 19 July 2021, theguardian.com/news/2021/jul/19/edward-snowden-calls-spyware-trade-ban-pegasus-revelations.

[41] Craig Timberg, Michael Birnbaum, Drew Harwell and Dan Sabbagh, "On the list: Ten prime ministers, three presidents and a king", *The Washington Post*, 20 July 2021, washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware.

[42] For example, the work of the UN Group of Governmental Experts, and the Open-ended working group on developments in the field of information and telecommunications in the context of international security. See Michael Schmitt, "The Sixth United Nations GGE and International Law in Cyberspace", *Just Security*, 10 June 2021, justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace; United Nations Office for Disarmament Affairs, *Open-ended Working Group*, un.org/disarmament/open-ended-working-group; United Nations Office for Disarmament Affairs, *Developments in the field of information and telecommunications in the context of international security*, un.org/disarmament/ict-security.

[43] UN Special Rapporteur on extrajudicial, summary or arbitrary executions, Annex to the Report: *Investigation into the unlawful death of Mr. Jamal Khashoggi*, 19 June 2019, UN Doc. A/HRC/41/CRP.1.

something close to impunity". Further, the UN mandate holder notes "[i]t is insufficient to say that a comprehensive system for control and use of targeted surveillance technologies is broken. It hardly exists."[44]

This culture of impunity is based on the purpose and promise of the technology itself: the act is invisible (unlike conventional tools, the technology is designed to prevent awareness or evidence of the targeting); there are few genuinely enforced constraints of operation; attribution is extremely difficult to establish (the technology is designed to obfuscate identity of the operator); vast surveillance capabilities are within reach regardless of the client's own technical sophistication. State actors thus operate without restraint and without real expectation of repercussion. One need look no further than the breadth of targeting uncovered through the Pegasus Project stories (see discussion above) to understand that impunity.

While NSO Group denies that it had insight into the targets uncovered in the Pegasus Project investigation, multiple new cases have been found in countries with known unlawful surveillance programmes, and even in countries where abuses of NSO Group software have previously been revealed. This shows that even if NSO Group had no knowledge of the specific abuses linked to its product, in these circumstances, it ought reasonably to have known that abuse would occur.[45]

[44] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report: *Surveillance and Human Rights*, 28 May 2019, UN Doc. A/HRC/41/35, para. 6 and 46.

[45] As explained in the Guidance to the United Nations' Ten Principles of the UN Global Compact, complicity for corporations means "being implicated" in human rights abuses. It is "generally" made up of two elements: an act by a company or its representative that "helps" another "in some way, to carry out a human rights abuse" and the "knowledge by the company that its act or omission could provide such help". This formulation requires only that the corporate act facilitate human rights abuses but does not mandate that the aid be substantial or a "but for" cause of the abuse. It also finds complicity based on knowledge that the aid *could* facilitate human rights abuse, without any requirement that the corporation know that it will in fact facilitate these abuses. United Nations Global Compact, "Principle Two: Human Rights", *The Ten Principles of the UN Global Compact*, unglobalcompact.org/what-is-gc/mission/principles/principle-2.

Corporations cannot escape complicity by wilful blindness. Instead, corporate knowledge can be deduced based on evidence of what was generally known, and thus what a reasonable corporation should know and likely in fact does know. The inquiry is comparable to that used to determine corporate negligence: one asks whether "a reasonable person in the company's shoes, with the information reasonably available at the time, would have known that there was a risk that its action would harm a person. This means that [one] will look at both what the company itself knew, and what a reasonable company in its shoes would have known about the risk that harm would occur." Publicly available information, as well as information brought to the attention of the company, is relevant in determining a company's knowledge. The company need not know the "full extent of the gross human rights abuses to which it contributes, provided some of the abuses are known." International Commission of Jurists (ICJ), *Report of the ICJ Expert Legal Panel on Corporate Complicity in International Crimes*, 1 January 2008, icj.org/report-of-the-international-commission-of-jurists-expert-legal-panel-on-corporate-complicity-in-international-crimes, at 20-22.

CORPORATE COMPLICITY UNDER INTERNATIONAL LAW AND STANDARDS

Complicity – as a legal concept – takes several forms, from individual criminal or civil liability as defined in domestic legal systems, to international criminal law involving corporate involvement in international crimes.

For the purposes of this briefing, we use the term "complicity" to be understood according to evolving norms of international law and standards applicable to private companies – or "legal persons", as they may be described in domestic legal systems.

The principle has evolved and is reflected in several leading international standards, variously applicable to international crimes, and other human rights harms. The commentary on the UN Global Compact makes clear that complicity in this context contains two primary elements:

- "An act or omission (failure to act) by a company, or individual representing a company, that "helps" (facilitates, legitimizes, assists, encourages, etc.) another, in some way, to carry out a human rights abuse, and
- The knowledge by the company that its act or omission could provide such help."[46]

It continues, for the avoidance of doubt: "[s]hould a corporation benefit from violations by the authorities, or entice, encourage or support them in violating human rights, corporate complicity would be evident."[47]

Whether or not the evident complicity of NSO Group in state human rights violations amounts to a grounds for civil or criminal liability under domestic, regional or international systems is a question to be answered by states, who owe an obligation of remedy to the victims of violations revealed in the Pegasus Project.

The Pegasus Project uncovered new evidence of a Pegasus spyware infection targeting Moroccan targets, despite NSO Group software having been discovered being used against Moroccan journalist Omar Radi in 2020.[48] Similarly, while NSO Group denies involvement in the murder of Jamal Khashoggi, the investigation found attempts to infect the phone of his wife prior to his murder, and its use to infect the phone of his fiancée even after his killing.[49] At least six dissidents associated with Rwanda were reportedly notified in 2019 by WhatsApp that they had been targeted by Pegasus spyware, and now new revelations reveal ongoing infections of Rwandans, including of the daughter of jailed activist Paul Rusesabagina, Carine Kalimba.[50]

Elsewhere, even where proof of past violations linked to NSO Group has not been found, such as in Azerbaijan, the severity of past surveillance-related violations should have put the company on notice of the risks to human rights. For example, Amnesty International has previously documented cases of surveillance of Azerbaijani human rights defenders at home and abroad.[51] The practice of using personal or intimate

[46] United Nations Global Compact, "Principle Two: Human Rights", *The Ten Principles of the UN Global Compact*, unglobalcompact.org/what-is-gc/mission/principles/principle-2.

[47] Andrew Clapham, "On Complicity" in M. Henzelin and R. Roth (editors), *Le droit penal a l'epreuve de l'internationalisation*, 2002, ssrn.com/abstract=1392988, pp. 241-275.

[48] Amnesty International, "Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group's Tools", 22 June 2020, amnesty.org/en/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools.

[49] Dana Priest, Souad Mekhennet and Arthur Bouvart, "Jamal Khashoggi's wife targeted with spyware before his death," *The Washington Post,* 18 July 2021, washingtonpost.com/investigations/interactive/2021/jamal-khashoggi-wife-fiancee-cellphone-hack.

[50] Stephanie Kirchgaessner, "Hotel Rwanda activist's daughter placed under Pegasus surveillance", *The Guardian*, 19 July 2021, theguardian.com/news/2021/jul/19/hotel-rwanda-activist-daughter-pegasus-surveillance.

[51] Amnesty International, "Activists targeted by 'Government Sponsored" Cyber Attack", 10 March 2017, amnesty.org/en/latest/news/2017/03/azerbaijan-activists-targeted-by-government-sponsored-cyber-attack.

images against women human rights defenders (WHRDs) to attempt to silence them is well documented[52] – which should have given more than adequate notice to NSO Group of the risks of this sale. And yet, that warning was ignored. The case of NSO Group demonstrates that even companies that know or should have known of abuses continue to supply their surveillance technology, and again, face few consequences.

NSO Group claims to have no insight into the targets selected by clients. But this is no answer. The evident failure to take note of the easily knowable risks of selling surveillance tools to the clients reveals a shocking failure to carry out due diligence on the company's part. A company may not avoid responsibility through such "wilful blindness" to risks of their sales and products and as reasonable person would appreciate.[53]

Reporting indicates that the Israeli authorities have launched an investigation into the revelations brought by the Pegasus Project. [54] Amnesty International urges the Israeli authorities to immediately revoke all export licences issued to NSO Group and ensure that their investigation is independent, impartial, and transparent, capable of determining the extent of unlawful targeting, to culminate in public statement on results of efforts and steps to prevent future harm.

States have chosen to preserve their flexibility to conduct offensive digital operations, and utilize the private sector to augment their surveillance capacity, to the detriment of individuals targeted with invasive surveillance, the digital environment as a whole, and even long-term state security interests. Meanwhile surveillance companies like NSO Group appear to have embraced complicity in pursuit of greater revenues. Their sales and products have enabled widespread violations, and evidence of this risk was readily available, whether they chose to take note of it or not. International human rights standards are designed to prevent the outsourcing of human rights responsibilities specifically in situations where the lines of the state/corporate nexus become blurred. Indeed, even confronted with these shocking disclosures, it is still uncertain whether states will hold each other to account, or whether NSO Group will ultimately face real consequences.

[52] Amnesty International, "Azerbaijan: Stop the vicious campaign of gendered smears and reprisals against women activists", 12 May 2021, amnesty.org/en/latest/news/2021/05/azerbaijan-stop-the-vicious-campaign-of-gendered-smears-and-reprisals-against-women-activists.

[53] International Commission of Jurists (ICJ), *Report of the ICJ Expert Legal Panel on Corporate Complicity in International Crimes*, 1 January 2008, §2.2.4, icj.org/report-of-the-international-commission-of-jurists-expert-legal-panel-on-corporate-complicity-in-international-crimes.

[54] Dan Williams, "Israel appoints task force to assess NSO spyware allegations – sources", *Reuters*, 21 July 2021, reuters.com/technology/israels-national-security-council-looking-into-nso-spyware-allegations-2021-07-21.

3. CONCLUSIONS AND RECOMMENDATIONS

The newly released disclosures concerning NSO Group demonstrate the urgent need for regulation and for a radical change in states' targeted digital surveillance practices and the participation of the private sector in those practices. Such necessary changes include:

INDEPENDENT OVERSIGHT OF BOTH THE SURVEILLANCE TRADE AND STATES' SURVEILLANCE PRACTICES

What happens when governments lacking independent oversight and accountability mechanisms get hold of these tools is no mystery: they use them to consolidate power at the expense of human rights, which the most recent disclosures make irrefutable. It should come as no surprise that governments using the tool to violate human rights have likewise felt free to turn these same tools against other states, undermining human rights there as well. While NSO Group claims its tools are used solely to lawfully investigate terrorism-related conduct and other crimes, it is more painfully obvious than ever that the company does not have the will and/or capacity to actually ensure that outcome. Yet companies do have an independent responsibility to respect human rights, regardless of the position or actions of the government where they operate or are based. This responsibility has been clearly articulated in the UN Guiding Principles, which state that "it exists independently of States' abilities and/or willingness to fulfil their own human rights obligations, and does not diminish those obligations. And it exists over and above compliance with national laws and regulations protecting human rights." It is clear that this is not happening, and that it is past time for robust oversight mechanisms, laws and regulation tailored to targeted digital surveillance.

A PATH TO REMEDY FOR INDIVIDUALS TARGETED IN VIOLATION OF THEIR HUMAN RIGHTS

We are only beginning to grasp the full extent and severity of the human rights impacts of this technology, as uncovered in these stories. Any such individual targeted in violation of their internationally recognized human rights, including those whose stories have now come to light, requires accessible paths to remedy. As the UN Guiding Principles on Business and Human Rights make clear, "[u]nless States take appropriate steps to investigate, punish and redress business-related human rights abuses when they do occur, the State duty to protect can be rendered weak or even meaningless."[55] Yet remedy has proven inordinately challenging in the context of digital surveillance, given the secrecy associated with surveillance operations, and the technical and legal obstacles to obtaining evidence or engaging in legal action against states or private surveillance companies. States must support the efforts of those impacted to seek justice and remedy – from both surveilling states and the companies that supply them – and take steps to deter future surveillance of

[55] UN High Commissioner for Human Rights (UNHCHR), *Guiding Principles on Human Rights, Implementing the United Nations 'Respect, Protect and Remedy Framework*, 2011, Principles 4 and 5.

these individuals, including by establishing causes of action under domestic law and international normative standards specific to targeted digital surveillance.[56]

GREATER TRANSPARENCY

Rather alarmingly in the face of these disclosures, the trend in the surveillance industry at present is toward reduced – not enhanced – transparency. Technical developments in spyware operation, such as incorporation of zero-click infection and network injection, are pushing awareness of and visibility into targeted attacks further out of reach. At the same time, private investment in the surveillance industry, through private equity or other private funds, compound the lack of independent oversight.[57]

While NSO Group released a first *Transparency and Responsibility Report* in June 2021, the report merely serves to illustrate the limits of the surveillance industry's tolerance of transparency. It cites certain limited statistics without explaining the context or implications of those figures, and provides few details concerning the practical application or results of the company's human rights due diligence, risk mitigation, or grievance mechanisms. It neglects to discuss past and active litigation against the company, or publicly reported findings concerning misuse of its products. It also asserts that "the sphere in which we operate requires that some key details, particularly direct identification of our customers or potential customers, remain confidential due to strict contractual and national security considerations."[58]

Transparency is a key aspect of the corporate responsibility to respect human rights, as articulated by the UN Guiding Principles. These state that businesses must have in place "policies and processes through which they can both know and show that they respect human rights in practice. Showing involves communication, providing a measure of transparency and accountability to individuals or groups who may be impacted and to other relevant stakeholders, including investors." The industry has failed to engage in meaningful transparency efforts. States and the public must act now to counter these trends.

Accordingly, Amnesty International recommends the following:

All states should:

a. Impose an immediate moratorium on the sale, transfer, and use of spyware technology. Given the breadth and scale of these findings, there is an urgent need to halt activities of states and companies, until there is a robust human rights regulatory framework in place.

b. Conduct an immediate, independent, transparent and impartial investigation of any cases of unlawful surveillance revealed by the Pegasus Project, and where appropriate, pursue legal avenues to provide remedies to victims and hold perpetrators to account, in accordance with international human rights standards.

c. Conduct an immediate, independent, transparent and impartial investigation into all export licences granted for spyware technology and revoke all marketing and export licences in situations where there is a substantial risk such technology could contribute to human rights violations.

d. 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.

---

[56] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report: *Surveillance and Human Rights*, 28 May 2019, UN Doc. A/HRC/41/35, §III.D.

[57] See Amnesty International and others, *Operating from the Shadows: Inside NSO Group's Corporate Structure*, (Index: DOC 10/4182/2021), 31 May 2021, amnesty.org/download/Documents/DOC1041822021ENGLISH.PDF.

[58] NSO Group, *Transparency and Responsibility Report 2021*, 30 June 2021, p. 4.

e. Adopt and enforce a legal framework requiring transparency by private surveillance companies, including information on self-identification/registration; products and services offered and sales.

f. Ensure that all companies domiciled in their territories are required to act responsibly and are held liable for their negative human rights impacts. States must require by law that these companies undertake human rights due diligence measures in respect of their global operations. This should include liability for harm caused and access to remedy in the home states of the companies, for affected communities. States should therefore initiate or support domestic proposals for corporate accountability legislation.

g. Disclose information about all previous, current and future contracts with private surveillance companies by responding to requests for information or by making proactive disclosures.

h. Furthermore, States must, at a minimum, implement the below recommendations if the moratorium on the sale and transfer of spyware equipment is to be lifted:

    a. Regulate the export of surveillance technologies, including to:

        i. Ensure the denial of export authorizations 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 account of 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.

        ii. Ensure that all relevant technologies are scrutinized for human rights risks prior to transfer as part of the licensing assessment.

        iii. 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.

        iv. Reform any existing legislation that imposes overly broad restrictions on disclosures of such information.

        v. Ensure that encryption tools and legitimate security research are not subject to export controls.

        vi. Implement domestic legislation that imposes safeguards against human rights violations and abuses through digital surveillance and establishes accountability mechanisms designed to provide victims of surveillance abuses a pathway to remedy.

        vii. Implement procurement standards restricting government contracts for surveillance technology and services to only those companies which demonstrate that they respect human rights in line with the UN Guiding Principles and have not serviced clients engaging in surveillance abuses.

        viii. 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.

    a. As a condition to continued operation of surveillance companies, demand immediate establishment of independent, multi-stakeholder oversight bodies for this and every

private surveillance company. This should include human rights groups and other civil society actors.

b. Establish community public oversight boards to oversee and approve the acquisition or use of new surveillance technologies, with powers to approve or reject based on the states' human rights obligations, provisions for public notice and reporting.

c. Reform existing laws that posed barriers to remedy for victims of unlawful surveillance and ensure that both judicial and non-judicial paths to remedy are available in practice.

Israel, Bulgaria, or other states in which NSO has corporate presence

a. Exporting States, including Israel and Bulgaria, should immediately revoke all marketing and export licences issued to NSO Group and conduct an independent, impartial, transparent investigation to determine the extent of unlawful targeting, to culminate in public statement on results of efforts and steps to prevent future harm.

NSO Group and its main investor Novalpina Capital should, at a minimum:

a. Immediately terminate the use, support and sale of Pegasus in states where the cyber surveillance software has been misused to unlawfully target HRDs, journalists and civil society as exposed through the Project Pegasus investigation.

b. Provide adequate compensation or other forms of effective redress to victims of unlawful surveillance using NSO Group's products.

c. Urgently take proactive steps to ensure that it does not cause or contribute to human rights violations, and to respond to any human rights violations – including those that feature in the Project Pegasus investigation – when they do occur. In order to meet that responsibility, NSO Group must carry out adequate human rights due diligence and take steps to ensure that HRDs, journalists and civil society do not continue to become targets of unlawful surveillance.

d. Terminate or suspend its contracts with governments who have used its tools to carry out unlawful targeted surveillance or otherwise violate human rights.

e. Ensure transparency regarding the volume, nature, value, destination, and end user of its surveillance technology transfers.

NSO Group Investors should:

a. Ensure that they do not contribute to human rights violations by way of their stake in private surveillance companies such as NSO Group. They should do this by demanding robust transparency and human rights due diligence, as well as accountability from NSO Group.

b. 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.

c. 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.

d. Exercise leverage on portfolio surveillance companies to ensure that the companies implement all the aforementioned recommendations applicable to them.

The private targeted surveillance industry should:

a. Conduct and publicly disclose robust human rights due diligence for all proposed transfers of surveillance technology.

b. Refrain from exporting surveillance technology if there is a substantial risk of human rights violations by end users.

c. Ensure transparency with regard to sales and contracts.

d. Conduct consultations with rights holders in destination countries before signing contracts to identify and assess human rights risks and develop mitigation measures.

e. Ensure public commitments to human rights as part of company policy.

f. Implement contractual protections against human rights abuses.

g. Implement design and engineering choices that incorporate human rights standards and safeguards.

h. Ensure regular audits into verification processes, the results of which are publicly disclosed.

i. Have an adequate notification process for reporting misuse of technology and grievance mechanisms.

j. Implement robust mechanisms for compensation or other forms of redress for victims of unlawful surveillance.

k. Adhere to the UNGPs and the Organization for Economic Cooperation and Development (OECD) Guidelines.

Investors in surveillance companies should:

a. Institute comprehensive human rights due diligence as part of the pre-investment due diligence process, and on an ongoing basis.

b. 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.

c. 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.

d. Exercise leverage on portfolio surveillance companies to ensure that the companies implement all the aforementioned recommendations applicable to them.

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

UNCOVERING THE ICEBERG

THE DIGITAL SURVEILLANCE CRISIS WROUGHT BY STATES AND THE PRIVATE SECTOR

The Pegasus Project is a collaborative investigation involving more than 80 journalists from 17 media organizations in 10 countries, coordinated by Forbidden Stories with technical support from Amnesty International. The disclosures have revealed how states' use of the targeted digital surveillance tools supplied by NSO Group is utterly out of control, destabilizing and threatening to individuals' human rights, including physical safety.

The stories published as a result of this collaboration speak for themselves. In this briefing, Amnesty International's goal is to contribute to the discussion by highlighting key insights from the perspective of international law that come out of the reporting and technical analyses. These include: the improper breadth of targeting under international human rights law; the clandestine nature of the tool that facilitates its illegal use and operation; the severe human rights violations that have resulted; the total impunity of states and companies in deploying this tool; and the failure of states to fulfil their obligation to protect their residents from illegal hacking and surveillance.

Finally, Amnesty International puts forward recommendations on the way forward, given the demonstrated need for independent oversight of the targeted digital surveillance industry, accountability for human rights violations and abuses, and greater transparency.

INDEX: DOC 10/4491/2021
JULY 2021
LANGUAGE: ENGLISH
amnesty.org

AMNESTY INTERNATIONAL