BEFORE THE BANGKOK CIVIL COURT

Jatupat Boonpattararaksa V NSO Group Technologies Ltd.(Black Case No. Por 3370/2566).

AMICUS CURIAE BRIEF ON BEHALF OF AMNESTY INTERNATIONAL

3 SEPTEMBER 2024

I. INTRODUCTION

1. In July 2022, an investigation, published by the Citizen Lab, a Canadian research institute based at the University of Toronto, in collaboration with the NGOs iLaw and Digital Reach, concluded that at least 30 Thai individuals were infected with NSO Group Technologies' (NSO Group) Pegasus spyware between October 2020 and November 2021.[1] One of the individuals infected with the NSO Group'sPegasus spyware was the Plaintiff, Jatupat Boonpattararaksa.

2. On 13 July 2023, the Plaintiff, Mr Jatupat Boonpattararaksa, filed a case for Tort and Claim for Damages in the Thai Civil Court against NSO Group Technologies Ltd. The Plaintiff's case file alleges that "[b]etween June and July 2021, the Defendant controlled and/or used Pegasus Spyware to spy and hack into the system and access the information on the Plaintiff's electronic device, which is an Apple-branded iPhone mobile phone, and used it with the mobile phone number (+66) 94-356- 2363, which is a computer system that the Plaintiff sets a password for and has measures to prevent unauthorized access. Thus, this action breaches the law and violates the Plaintiff's right to privacy, freedom of communication, freedom of travel, and choice of residence."

3. Over the past decade, civil society organizations, researchers, and journalists have exposed how governments around the world have been unlawfully targeting activists, journalists, and politicians using tools developed by private cyber-surveillance companies. Compelling evidence shows a widespread misuse of these technologies for illegitimate purposes, often using "national security" as a pretext to justify targeting critical voices, journalists, human rights defenders (HRDs), and even politicians. Amnesty International and numerous civil society organizations have repeatedly warned that states' opaque trade and deployment of privately manufactured surveillance technologies, particularly spyware, have wrought a digital surveillance crisis, which has severely and detrimentally impacted human rights, media freedoms, and social movements across the world.

4. Accordingly, Amnesty International hereby submits an amicus curiae brief to the Bangkok Civil Court at Ratchadaphisek Road for the matter above, which seeks to assist the Court by drawing attention to a body of international human rights law and standards that the Court may wish to consider in its adjudication of the case. The amicus brief will largely make five points:

    4.1 First, there is a clear global consensus that business enterprises should respect all internationally recognized human rights wherever they operate. This responsibility is independent of a state's own human rights obligations and may require companies to go beyond what is required according to the applicable domestic law, which is described further below. Thailand recognizes that business enterprises should respect all internationally recognized human rights wherever they operate.
    4.2 Second, NSO Group has publicly recognized the application of international human rights standards to its operations.
    4.3 Third, NSO Group has been repeatedly alerted to allegations of human rights abuses related to the use of Pegasus but have failed to publicly provide any detailed information on due diligence processes, nor provided remedy to victims.
    4.4 Fourth, NSO Group has a responsibility to conduct human rights due diligence (HRDD) by effectively monitoring use of Pegasus to identify, prevent, mitigate, and account for adverse human rights impacts.
    4.5 Fifth, in line with its obligations under international human rights law, Thailand must protect individuals under its jurisdiction from human rights abuses, including by guaranteeing the right to privacy and the right to an effective remedy.

---

[1] Citizen Lab, *GeckoSpy: Pegasus Spyware Used against Thailand's Pro-Democracy Movement*, 17 July 2022, "https://citizenlab.ca/2022/07/geckospy-pegasus-spyware-used-against-thailands-pro-democracy-movement/; iLaw, *Parasite That Smiles: Pegasus Spyware Targeting Dissidents in Thailand*, 16 July 2022, https://www.ilaw.or.th/articles/35057. It must be noted that the Bangkok-based NGO iLaw, one of the organizations that led the forensic investigation with The Citizen Lab and Digital Reach, provided in the initial research report a list of 30 individuals whose devices were infected with Pegasus spyware. Shortly after, they revealed five additional cases of infections on devices belonging to members of the now-dissolved opposition party Move Forward and its affiliated political group Progressive Movement. See Citizen Lab, *GeckoSpy: Pegasus Spyware Used against Thailand's Pro-Democracy Movement* (previously cited) and iLaw, สิ่งที่เป็นภัยต่อเราอาจจะไม่ใช่สปายแวร์แต่คือพลเอกประยุทธ์" ถอดเทิ่ม การอภิปราย "เพกาซัส" ของพิจารณ์ เชาวพัฒนวงศ์, 21 July 2022, https://www.ilaw.or.th/articles/5314 (in Thai).

II. INTRODUCTION TO AMNESTY INTERNATIONAL

5. Amnesty International is a worldwide movement of 13 million people working for the respect, protection and fulfilment of internationally recognized human rights. The movement has members and supporters in more than 150 countries and territories including in Thailand and is independent of any government, political ideology, economic interest, or religion. Amnesty International bases its work on international human rights instruments adopted by the United Nations and regional bodies. Amnesty International Charity Ltd., a subsidiary of Amnesty International Ltd., is a registered charity in England and Wales (No. 294230). Amnesty International Ltd. has a regional office of the International Secretariat (No. 0-9940-01086-88-5) and a national section of the global movement, Amnesty International Thailand, located and registered in Bangkok (TOR. 405/2545), Thailand.

6. Amnesty International is recognized as an accurate, unbiased and credible source of research and analysis of human rights conditions around the world. Amnesty International conducts research and leads efforts to advance international human rights at the global, regional and national levels. Amnesty International has intervened in many cases that have raised a wide range of human rights issues before national and international courts.

7. This amicus curiae brief has been prepared and submitted by the International Secretariat of Amnesty International Limited, registered in England and Wales. The International Secretariat of Amnesty International has a particular interest in the application of international human rights law and standards on how the use of technology interacts and/or undermines human rights. This work is primarily done by Amnesty International's Technology Programme (Amnesty Tech), as well as a team focused on Business and Human Rights (BHR) issues. The amicus curiae submission builds on Amnesty International's work on highly invasive spyware and other rights-threatening surveillance technologies which have been used to target HRDs, journalists and other members of civil society worldwide and how multiple countries have failed to regulate the use of these technologies and protect individuals from its human rights harms.

III. INTERNATIONAL LAW AND STANDARDS

8. Under international law, the obligation to ensure that human rights are respected, protected and fulfilled rests with the state, including the legislative, executive and judicial branches. Thailand is a party to eight of the nine principal international treaties on human rights, including the International Covenant on Civil and Political Rights (ICCPR).[2] Thailand acceded to the ICCPR on 29 October 1996.[3] Under the principle of *pacta sunt servanda* and general principles governing the law of treaties, Thailand is bound to apply in good faith all international treaties to which it is a party.[4] Therefore, Thailand may not rely on provisions of its internal law to justify a failure to meet a treaty obligation.[5]

9. All United Nations (UN) human rights treaties provide for the obligation of states to take appropriate steps to protect persons from the arbitrary interference with their human rights by non-state actors, including business enterprises.[6] States must abide by this obligation with respect to any business that has operations in its territory

[2] Apart from the International Covenant on Civil and Political Rights (ICCPR), Thailand has ratified other principle human rights treaties including: (i) Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) and its Optional Protocol; (ii) Convention on the Rights of the Child (CRC) and its two Optional Protocols; (iii) International Convention on the Elimination of All Forms of Racial Discrimination (CERD); (iv) Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT); (v) Convention on the Rights of Persons with Disabilities (CRPD), and (vi) Convention for the Protection of All Persons from Enforced Disappearance (CED), and (vii) International Covenant on Economic, Social and Cultural Rights (ICESCR).

[3] Office of the High Commissioner for Human Rights (OHCHR), UN Treaty Body Database, https://tbinternet.ohchr.org/_layouts/15/TreatyBodyExternal/Treaty.aspx?CountryID=172&Lang=EN (accessed on 27 August 2024).

[4] United Nations, "Vienna Convention on the Law of Treaties", 23 May 1969, United Nations, Treaty Series, vol. 1155, at 331, Article 26, available at: https://www.refworld.org/docid/3ae6b3a10.html; UN Human Rights Committee (HRC), General Comment 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, 26 May 2004, UN Doc. CCPR/C/21/Rev.1/Add. 13, para. 3.

[5] UN, "Vienna Convention on the Law of Treaties" (previously cited), Articles 26 and 27; HRC, General Comment 31 (previously cited), para. 4.

[6] For example, UN Committee on Economic, Social and Cultural Rights (CESCR), General comment 24 (2017) on 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, para 14, available at https://www.refworld.org/docid/5beaecba4.html ('CESCR General Comment No. 24'); UN Committee on the Rights of the Child (CRC), General comment 16 on State Obligations Regarding the Impact of the Business Sector on Children's Rights, 17 April 2013, UN Doc

and/or subject to its jurisdiction, even if they are domiciled in other countries, to prevent them from causing or contributing to human rights abuses.[7]

10. The jurisprudence of UN treaty bodies to this effect went on to inform the development of the UN Guiding Principles on Business and Human Rights (UN Guiding Principles), which were endorsed unanimously by the UN Human Rights Council in 2011.[8] The UN Guiding Principles recognized the state's duty to protect against human rights abuses by business enterprises, including by taking appropriate steps to provide access to effective remedy to those affected, as among its three principal pillars.[9] Further, the UN Guiding Principles provide that business enterprises have a responsibility to respect all human rights, which will be described in further detail below.

State Obligations to respect the right to privacy

11. The right to privacy is enshrined in Article 12 of the UDHR. Article 17 of the ICCPR states that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence," and that "everyone has the right to the protection of the law against such interference or attacks".[10] The right to privacy must be guaranteed against all interferences and attacks from both state and non-state actors.[11]

12. The Human Rights Committee, which oversees the implementation of the ICCPR, has explained that the reference to 'unlawful' in Article 17 of ICPPR means that any interference with the right to privacy, including digital surveillance operations, can only take place on the basis of law, and such law must comply with the provisions, aims, and objectives of the ICCPR.[12] It must only be applied when necessary, proportionate and legitimate[13] and be subject to safeguards adequate to prevent abuse, such as being subject to judicial oversight for a defined purpose and period.[14] Furthermore, any limitation on the right to privacy must comply with the principle of non-discrimination and other rights recognized under international law.[15] Where the limitation does not meet these criteria, it is unlawful and/or arbitrary.[16]

13. Surveillance can be permissible for the "protection of people's lives or bodily integrity and the security of critical

---

CRC/C/GC/16, para. 28, available at https://www.refworld.org/docid/51ef9cd24.html ('CRC General Comment No. 16'); HRC, General Comment 31 (previously cited), para. 8; UN Committee on the Elimination of Discrimination against Women (CEDAW), 'Concluding observations on the combined fourth and fifth periodic reports of India', 24 July 2014, UN Doc. CEDAW/C/IND/CO/4-5, paras. 14-15, available at https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CEDAW/C/IN D/CO/4-5&Lang=En; UN Committee on the Elimination of Racial Discrimination (ICERD), 'Consideration of Reports Submitted by States Parties Under Article 9 of the Convention - Concluding observations of the Committee on the Elimination of Racial Discrimination: Canada', 25 May 2007, UN Doc CERD/C/CAN/CO/18, para. 17, available at https://undocs.org/CERD/C/CAN/CO/18.

[7] OHCHR, UN Guiding Principles on Business and Human Rights, Principle 1, 2011, https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf, p. 3; Amnesty International, *Injustice Incorporated: Corporate Abuses and the Human Right to Remedy* (Index: POL 30/001/2014), 7 March 2014, p. 22.

[8] The UN Guiding Principles are internationally recognized standards for both States and corporate actors in the context of business-related human rights abuses and should guide this Court's adjudication. See also UN Human Rights Council (UNHRC), Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, 13 February 2007, UN Doc. A/HRC/4/35/Add.1.

[9] OHCHR, UN Guiding Principles on Business and Human Rights (previously cited), Pillar I and III, Principle 1 and 25, pp. 3, 27.

[10] International Covenant on Civil and Political Rights (ICCPR), Article 17.

[11] HRC, CCPR, General Comment 16: Article 17 (Right to Privacy), adopted on 8 April 1988, para 1.

[12] HRC, General Comment 16: Article 17 (Right to Privacy) (previously cited), para 1.

[13] 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, www.undocs.org/A/HRC/41/35, para. 50(b).

[14] UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report: Surveillance and human rights (previously cited), para. 50(c).

[15] OHCHR, Report: *The Right to Privacy in the Digital Age*, 30 June 2014, UN Doc. A/HRC/27/37, paras 22-23.

[16] OHCHR, The Right to Privacy in the Digital Age (previously cited).

infrastructure", if conducted in line with the conditions mentioned above.[17] However, it is not permissible under international law to use surveillance for the purpose of tracking dissidents, HRDs, and members of marginalized communities based on their exercise of human rights, or protected characteristics.[18]

14. The right to privacy underpins other key rights for civic participation, such as freedom of expression and freedom of peaceful assembly and association. In the digital age, privacy and expression are intertwined with online privacy serving as a gateway to secure exercise of the freedom of opinion and expression.[19] The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has explained that the 'interference with privacy through targeted surveillance is designed to repress the exercise of the right to freedom of expression.'[20] The right to privacy includes the right of individuals to know who holds information about them and how that information is used.[21]

15. In line with the standards outlined above, states have an obligation to protect against arbitrary interference with the right to privacy by non-state actors, such as businesses. The use of highly invasive spyware such as Pegasus always constitutes a violation of the right to privacy under IHRL, even with human rights safeguards in place, because its functionality could not be limited or independently audited to ensure proportionality.[22] States must establish legislation banning the use of such highly invasive spyware; guarantee access to justice and effective remedy to victims of human rights violations resulting from such spyware; and regulate the operations of businesses related to spyware based on human rights law and standards. If the state fails to take appropriate steps to protect the privacy of individuals from interference by businesses, it has failed to comply with its duty under IHRL.

Corporate responsibility to respect the right to privacy and conduct Human Rights Due Diligence (HRDD)

16. Companies have a responsibility to respect human rights regardless of their size, sector, or where they operate, as reflected in the UN Guiding Principles. This responsibility to respect human rights is independent of a state's own human rights obligations and exists over and above compliance with domestic law.[23] The corporate responsibility to respect human rights includes the right to privacy.[24] To abide by this responsibility, businesses should avoid causing or contributing to human rights abuses and address any adverse human rights impacts if and when they occur.[25] Businesses should also use their leverage to prevent or mitigate adverse human rights impacts directly linked to their operations, products or services through their business relationships, even if they do not contribute to those impacts.[26]

17. The UN Guiding Principles stipulate that, as part of their responsibility to respect human rights, business enterprises should carry out Human Rights Due Diligence (HRDD) to "identify, prevent, mitigate and account for

[17] OHCHR, The Right to Privacy in the Digital Age (previously cited), para. 50.

[18] OHCHR, The Right to Privacy in the Digital Age (previously cited).

[19] Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report: *Surveillance and human rights*, (previously cited), para. 24.

[20] Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Report: *Surveillance and human rights*, (previously cited), para. 22.

[21] HRC, General Comment 16: Article 17 (Right to Privacy) (previously cited), 10.

[22] European Data Protection Supervisor, Preliminary Remarks on Modern Spyware, 15 February 2022, https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf, p. 8.

[23] UN Guiding Principles, Principle 11. This responsibility was expressly recognized by the UN Human Rights Council on 16 June 2011, when it endorsed the UN Guiding Principles, and on 25 May 2011 when the 42 governments that had then adhered to the Declaration on International Investment and Multinational Enterprises of the OECD unanimously endorsed a revised version of the OECD Guidelines for Multinational Enterprises. See UNHRC, Human Rights and Transnational Corporations and other Business Enterprises, Resolution 17/4, 6 July 2011, UN Doc. A/HRC/RES/17/4, available at daccess-ods.un.org/tmp/638279.914855957.html

[24] OHCHR, UN Guiding Principles on Business and Human Rights (previously cited), Principle 12, including Commentary, pp. 13-4.

[25] OHCHR, UN Guiding Principles on Business and Human Rights (previously cited), Principle 13(a), including Commentary.

[26] OHCHR, UN Guiding Principles on Business and Human Rights (previously cited), Principle 13(b), including Commentary.

how they address their adverse human rights impacts[.]"[27] HRDD has four main elements: identifying and assessing actual and potential adverse human rights impacts; integrating and acting upon the findings; tracking the effectiveness of their response; and communicating to affected stakeholders about how the company is addressing any adverse human rights impacts.[28] The scope of HRDD encompasses a business's entire value chain, both upstream and downstream, including the delivery of a product or license to use a product to the market and ultimately the end user.[29] HRDD should be an ongoing and dynamic process in recognition that human rights risks may change over time as the business enterprise's operations and operating context evolve.[30]

18. To understand the risks its business poses to human rights, companies should also adopt an intersectional understanding of discrimination and its particular manifestations in the contexts they operate within. In so doing, businesses should "pay special attention to any particular human rights impacts on individuals from groups or populations that may be at heightened risk of vulnerability or marginalization," including HRDs.[31]

19. Where a business enterprise identifies through due diligence that it may cause or contribute to a human rights abuse, it should cease or prevent its contribution to the adverse impact and, where applicable, use its leverage to mitigate any remaining impact to the greatest extent possible.[32] If a company has contributed to or caused a negative human rights impact, then it should provide remedy to those who have suffered the harm.[33] Transparency is a key component of human rights due diligence. The UN Guiding Principles make clear that companies need to "know and show that they respect human rights" and "showing involves communication, providing a measure of transparency and accountability to individuals or groups who may be impacted and to other relevant stakeholders."[34]

20. For the purposes of this case, Amnesty International respectfully brings to the attention of the court that the corporate responsibility to respect the right to privacy is of particular salience regarding technology-related businesses, such as cybersecurity firms or developers like NSO Group, given the direct link between its products and services, targets' data, and their privacy.[35]

21. The Office of the UN High Commissioner for Human Rights (OHCHR)'s B-Tech project, which provides authoritative guidance and resources for implementing the UN Guiding Principles in the technology space, has clarified that a technology company can contribute to an adverse human rights impact through its own activities when they are combined with those of other actors to cause harm, including by "facilitat[ing] or incentivis[ing] the user in such a way as to make the adverse human rights impact more likely."[36] OHCHR's interpretative guidance on the UN Guiding Principles states 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

---

[27] OHCHR, UN Guiding Principles on Business and Human Rights (previously cited), Principle 17.

[28] OHCHR, UN Guiding Principles on Business and Human Rights (previously cited), Principle 17; OHCHR, The Corporate Responsibility to Respect Human Rights: An Interpretive Guide (previously cited), pp. 31-35.

[29] If a business enterprise has large numbers of entities in their value chains, they should identify general areas where the risk of adverse human rights impacts is most significant and prioritize these for HRDD. OHCHR, UN Guiding Principles on Business and Human Rights (previously cited), Commentary to Principle 17.

[30] OHCHR, UN Guiding Principles on Business and Human Rights (previously cited), Principle 17.

[31] OHCHR, UN Guiding Principles on Business and Human Rights (previously cited), Principle 18, including Commentary.

[32] OHCHR, UN Guiding Principles on Business and Human Rights (previously cited), Principles 17 and 19.

[33] OHCHR, UN Guiding Principles on Business and Human Rights (previously cited), Principle 15(c).

[34] OHCHR, UN Guiding Principles on Business and Human Rights (previously cited), Commentary to Principle 21.

[35] OHCHR, The Corporate Responsibility to Respect Human Rights: An Interpretive Guide, 2012, https://www.ohchr.org/sites/default/files/Documents/publications/hr.puB.12.2_en.pdf, pp. 20-21 ("An information and communications technology company may be at particular risk of impacting the rights to privacy and/or information of its users as a result of data sharing or censorship").

[36] This excludes activities that have trivial or minor effect on the actions of the user. OHCHR, Access to remedy and the technology sector: basic concepts and principles: A B-Tech Foundational Paper, January 2021, https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/access-to-remedy-concepts-and-principles.pdf.

dissidents contrary to human rights".[37] Spyware is a form of intrusion software that interferes with a device's normal operation to collect information without alerting the user and sends it to another unauthorised entity, and therefore, by its very nature, any use to trace and prosecute political dissidents would constitute a human rights violation.

22. Business enterprises in the technology space should conduct human rights due diligence to ensure that their technology products and services are not directly linked to adverse human rights impacts through their business relationships, including government clients who are known to have a record of violating the right to privacy.[38] Businesses should also put in place clear policies and procedures for meeting their responsibility to respect human rights that are publicly available and reflected in operational policies and procedures, including with respect to the receipt, processing and retention of personal data with due regard to the right to privacy.[39]

The right to an effective remedy

23. The obligation to respect and implement international human rights law as entrenched in the respective bodies of law, includes, among others, the duty to "provide those who claim to be victims of a human rights or humanitarian law violation with equal and effective access to justice, …, irrespective of who may ultimately be the bearer of responsibility for the violation."[40] The right to an effective remedy is a "core tenet of international human rights law"[41] that is enshrined in customary international law.[42] The right to an effective remedy has been recognized under various international human rights treaties and instruments,[43] including the UDHR, the ICCPR, the CEDAW, and the CAT, also applicable in Thailand.[44]

24. The right to an effective remedy is comprised of three core elements: (i) access to justice, (ii) reparations (including restitution, compensation, rehabilitation, satisfaction and guarantees of non-repetition), and (iii) access to information.[45]

25. As access to remedy is a key pillar of the business and human rights framework, the UN Guiding Principles stipulate that where "business enterprises identify that they have caused or contributed to adverse impacts, they

---

[37] OHCHR, The Corporate Responsibility to Respect Human Rights: An Interpretive Guide (previously cited), p. 7.

[38] OHCHR, UN Guiding Principles on Business and Human Rights (previously cited), Principle 17, including Commentary. See also OHCHR, Human Rights Translated: A Business Reference Guide, 2008, https://www.ohchr.org/sites/default/files/Documents/Issues/Business/Human_Rights_Translated_web.pdf, p. 48.

[39] OHCHR, UN Guiding Principles on Business and Human Rights (previously cited), Principle 17, including Commentary OHCHR, Human Rights Translated: A Business Reference Guide (previously cited), p. 48. It is also important to note that Principle 21 of UN Guiding Principles also make clear that companies need to "know and show that they respect human rights" and "showing involves communication, providing a measure of transparency and accountability to individuals or groups who may be impacted and to other relevant stakeholders."

[40] UN General Assembly, Resolution 60/147: Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law, adopted on 16 December 2005, UN Doc. A/RES/60/147, https://www.ohchr.org/sites/default/files/2021-08/N0549642.pdf.

[41] UN High Commissioner for Human Rights, Report: *Improving accountability and access to remedy for victims of business-related human rights abuse* (previously cited), para. 6.

[42] See International Criminal Tribunal for Rwanda, *Prosecutor v. André Rwamakuba*, Case ICTR-98- 44C, Decision on Appropriate Remedy, 31 January 2007, para. 40; International Criminal Tribunal for Rwanda, *Prosecutor v. André Rwamakuba*, Case ICTR98-44C-A, Decision on Appeal Against Decision on Appropriate Remedy, 13 September 2007, paras 23-25; Inter-American Court of Human Rights, *Cantoral-Benavides v. Perú*, 2001. (ser.C) No. 88, at para. 40.

[43] Universal Declaration of Human Rights (UDHR), Article 8; ICCPR, Article 2(3); ICESCR Article 2;CERD, Article 6; CEDAW, Article 2; CAT, Article 14; European Convention on Human Rights, Article 13; American Convention on Human Rights, Article 25; African Charter on Human and Peoples' Rights, Article 7(1)(a); Charter of Fundamental Rights of the European Union, Article 47; Arab Charter on Human Rights, Articles 12 and 23; UN General Assembly, *Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law* (previously cited), among others.

[44] Thailand ratified CAT in 2007. See: OHCHR, UN Treaty Database (previously cited), (accessed on 28 August 2024).

[45] See UN General Assembly, *Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law* (previously cited), Principle 11 "Victims right to remedies."

should provide for or cooperate in their remediation through legitimate processes."[46] Additionally, although the state is the ultimate guarantor of the right of access to remedy, businesses can adversely affect the full enjoyment of this right "if, for example, an enterprise obstructs evidence or interferes with witnesses."[47]

26. Accordingly, Thailand has a duty to create an accountability framework that provides equal and effective access to justice for all; establishes mechanisms for effective, prompt, thorough, and impartial investigations, including access to relevant information; and offers adequate, prompt, and effective reparations including non-repetition guarantees for human rights abuses.[48]

27. With respect to the provision of remedial processes, Principle 25 of the UN Guiding Principles acknowledge the obligation of States to "take appropriate steps to ensure, through judicial, administrative, legislative or other appropriate means, that when such abuses occur within their territory and/or jurisdiction those affected have access to effective remedy."[49] These include State-based judicial or, for certain transgressions, nonjudicial grievance mechanisms.[50]

IV. OBSERVATIONS ON THE SIGNIFICANCE OF SUCH INTERNATIONAL LAW AND STANDARDS

Thailand recognizes that business enterprises should respect all internationally recognized human rights wherever they operate.

28. As outlined in the section above, there is a clear international consensus that companies should respect all human rights wherever they operate, particularly under the UN Guiding Principles.

29. Several steps have been taken by the Thai government toward greater regulation of businesses concerning the respect of human rights. These steps include the adoption of a National Action Plan on Business and Human Rights (BHR NAP). The UN Working Group on Business and Human Rights urges all States to create, implement, and regularly update a BHR NAP a as part of their obligation to promote and enforce the UN Guiding Principles. This initiative is essential to advancing efforts to ensure companies respect human rights, are held accountable for violations, and that victims of corporate abuses have access to justice.[51]

30. Thailand's First BHR NAP (2019-2022), adopted on 29 October 2019,[52] was founded primarily upon the UN Guiding Principles. This first BHR NAP itself explains that its drafting process derives from the attempt to contextualize the UN Guiding Principles to the situation of Thailand.[53] The protection of HRDs was one of the four priority areas under this national policy.

---

[46] OHCHR, UN Guiding Principles on Business and Human Rights (previously cited), Principle 22, including Commentary.

[47] OHCHR, The Corporate Responsibility to Respect Human Rights: An Interpretive Guide (previously cited), p. 13 (although the source cited refers to adverse effects on the right to a fair trial, such conduct can also impinge on other rights such as the right of access to remedy as addressed here).

[48] See: Corte Interamericana de Derechos Humanos (IDH), Cuadernillos de Jurisprudencia de la Corte Interamericana de Derechos Humanos [Inter-American Court of Human Rights Precedent Books], No. 13: Protección Judicial, 2021, https://www.corteidh.or.cr/sitios/libros/todos/docs/cuadernillo13_2021.pdf (in Spanish);; Antônio A. Cançado Trindade, El derecho de acceso a la justicia internacional y las condiciones para su realización en el sistema interamericano de protección de los derechos humanos [The right of access to international justice and the conditions for its implementation in the inter-American system for the protection of human rights], OEA/Ser.GCP/doc.3654/02, 2002, https://www.corteidh.or.cr/tablas/r08066-2.pdf (in Spanish).

[49] OHCHR, UN Guiding Principles on Business and Human Rights (previously cited), Principles 25-30. Additionally, businesses should provide operational-level grievance mechanisms and cooperate with industry-level and State-provided grievance mechanisms to ensure access to effective remedies for those affected.

[50] OHCHR, UN Guiding Principles on Business and Human Rights (previously cited), Principles 25-30.

[51] International Commission of Jurists (ICJ), "Thailand: Government and companies must effectively implement commitments under the National Action Plan on Business and Human Rights", 20 September 2022, https://www.icj.org/thailand-commitments-on-business-and-human-rights/

[52] Thailand Ministry of Justice Rights and Liberties Protection Department, First National Action Plan on Business and Human Rights (2019–2022) ("First NAP B&HR"), October 2019, https://www.ohchr.org/sites/default/files/Documents/Issues/Business/NationalPlans/NAPThailandEN.pdf

[53] Thailand Ministry of Justice Rights and Liberties Protection Department, First NAP B&HR (previously cited).

31. The Second BHR NAP (2023-2027) was endorsed by the Thai Cabinet on 25 July 2023.[54] Similar to the first BHR NAP, this version also prioritizes the protection of HRDs. It highlights the importance of "assessing, issuing, reviewing, improving or revising laws, measures, mechanisms, and procedures for protecting human rights defenders, including human rights defenders who are women or part of other vulnerable groups, to ensure they could work safely both offline and online in line with international human rights law and standards." [55], as well as "providing remedy for victims / injured parties in line with the law and develop measures for appropriate and gender-sensitive physical and mental remedies in accordance with international human rights standards, including the UN Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power".[56]

NSO has publicly recognized the application of international human rights standards in carrying out its operations.

32. NSO Group's Human Rights Policy, available online, provides that: "We are committed to respecting human rights as enshrined in the International Bill of Human Rights and the principles concerning fundamental rights set out in the International Labor Organization's Declaration on Fundamental Principles and Rights at Work. The United Nations Guiding Principles on Business and Human Rights guide us in fulfilling our obligation to respect human rights throughout our business activities".[57]

33. In June 2018, an Amnesty International staff member was targeted with a malicious WhatsApp message which carried links that Amnesty International believes are used to distribute and deploy sophisticated mobile spyware. The suspicious domains used in this case overlap with infrastructure that had previously been identified as part of the Pegasus spyware platform. In response, NSO Group stated to Amnesty International: "NSO Group develops cyber technology to allows government agencies to identify and disrupt terrorist and criminal plots. Our product is intended to be used exclusively for the investigation and prevention of crime and terrorism. Any use of our technology that is counter to that purpose is a violation of our policies, legal contracts, and the values that we stand for as a company. If an allegation arises concerning a violation of our contract or inappropriate use of our technology, as Amnesty has offered, we investigate the issue and take appropriate action based on those findings. We welcome any specific information that can assist us in further investigating of the matter". [58]

34. NSO also affirms its responsibility to conduct human rights due diligence and take appropriate steps to prevent and mitigate harms through the use of its products, including Pegasus spyware: "In our sales process, we thoroughly evaluate the potential for adverse human rights impacts arising from the misuse of our products by considering, among other factors, the specific customer, the proposed customer use case and the past human rights performance and governance standards of the country involved."[59]

35. Although NSO Group acknowledges the UN Guiding Principles to be an "authoritative international standard", Amnesty International respectfully brings to the attention of this court that it is not clear how, in practice, NSO Group complied with these principles and whether it conducted adequate human rights due diligence regarding whether its products and services are directly linked to adverse human rights impacts by the company's business

---

[54] ICJ, "Thailand: Legal and practical barriers frustrate access to effective remedies for human rights abuses involving Thai transnational corporations abroad", 16 August 2023, https://www.icj.org/thailand-legal-and-practical-barriers-frustrate-access-to-effective-remedies-for-human-rights-abuses-involving-thai-transnational-corporations-abroad/

[55] Thailand Ministry of Justice Rights and Liberties Protection Department, Second National Action Plan on Business and Human Rights ("Second NAP B&HR"), September 2023, https://globalnaps.org/wp-content/uploads/2024/01/NAP-Thailand-2023-2027-Thai.pdf, p. 125 (in Thai).

[56] Thailand Ministry of Justice Rights and Liberties Protection Department, ("Second NAP B&HR") (previously cited), p. 136.

[57] NSO Group, Human Rights Policy, September 2019, https://www.nsogroup.com/wp-content/uploads/2019/09/NSO-Human-Rights-Policy_September19.pdf, para. 1.

[58] Statement by NSO Group received on 31 July 2018. Amnesty International, *Amnesty International Among Targets of NSO-powered Campaign*, 1 August 2018, https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/

[59] NSO Group, Human rights policy (previously cited), para. 1.

relationships, particularly with its clients.[60] This is discussed further below.

NSO has been repeatedly alerted to allegations of human rights abuses related to the use of Pegasus.

36. NSO Group's website states that "NSO products are used exclusively by government intelligence and law enforcement agencies to fight crime and terror". [61] However, a series of published reports have alleged the use of Pegasus spyware against human rights defenders and journalists in numerous locations around the world. In the most high-profile investigation, The Pegasus Project in 2021, numerous cases of targeting of journalists and human rights defenders were documented globally.[62] Aside from the 2021 Pegasus Project, there have been many reports, backed by digital forensic research, of Pegasus spyware, being used against journalists and human rights defenders in numerous countries, including in Bahrain,[63] El Salvador[64], India,[65] Jordan,[66] and Mexico.[67]

37. In response to the Pegasus Project revelations in 2021, NSO Group responded to say that it "will continue to investigate all credible claims of misuse and take appropriate action based on the results of these investigations"[68] However, NSO Group has not released the details of any subsequent investigations of misuse against individuals. Furthermore, NSO Group has not disclosed the details of any due diligence processes in relation to any cases of misuse, nor disclosed any cases of remedy provided to human rights defenders or journalists who have been targeted with Pegasus.

38. In the case of Thailand, the use of Pegasus against human rights defenders and journalists was first reported on by Citizen Lab, iLaw and Digital Reach in July 2022; this report included the use of Pegasus against the Plaintiff[69]. Furthermore, in April 2023, four UN Special Rapporteurs wrote to the Thai government raising concerns about the use of Pegasus spyware and the government's failure to protect those allegedly subjected to unlawful surveillance.[70] They requested information from the government, including on "the measures in place to ensure the protection of the rights to privacy, to freedom of expression and to freedom of peaceful assembly of the 35 above-mentioned individuals, as well as any other person in Thailand, subjected to spyware surveillance".[71]

---

[60] See NSO Group, Transparency and Responsibility Report 2023, 31 December 2023, https://www.nsogroup.com/wp-content/uploads/2023/12/2023-Transparency-and-Responsibility-Report.pdf

[61] NSO Group, "About Us", https://www.nsogroup.com/about-us/ (accessed on 27 August 2024).

[62] The Pegasus Project was a collaboration by more than 80 journalists from 17 media organizations in 10 countries coordinated by Forbidden Stories and for which Amnesty International was the technical partner. It followed the revelation of 50,000 phone numbers of potential surveillance targets around the world. Amnesty International, "Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally", 19 July 2021, https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/

[63] Citizen Lab, *Pearl 2 Pegasus: Bahraini Activists Hacked with Pegasus Just Days after a Report Confirming Other Victims*, 18 February 2022,

[64] Citizen Lab, *Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware*, 12 January 2022, https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/

[65] Amnesty International, *India: Damning new forensic investigation reveals repeated use of Pegasus spyware to target high-profile journalists*, 28 December 2023, https://www.amnesty.org/en/latest/news/2023/12/india-damning-new-forensic-investigation-reveals-repeated-use-of-pegasus-spyware-to-target-high-profile-journalists/

[66] Front Line Defenders, *Report: Jordanian Human Rights Defenders and Journalists Hacked with Pegasus Spyware*, 5 April 2022, https://www.frontlinedefenders.org/en/statement-report/report-jordanian-human-rights-defenders-and-journalists-hacked-pegasus-spyware

[67] Citizen Lab, *Breaking the News: New York Times Journalist Ben Hubbard Hacked with Pegasus after Reporting on Previous Hacking Attempts*, 24 October 2021, https://citizenlab.ca/2021/10/breaking-news-new-york-times-journalist-ben-hubbard-pegasus/

[68] Amnesty International, "Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally" (previously cited).

[69] Citizen Lab, *GeckoSpy: Pegasus Spyware Used against Thailand's Pro-Democracy Movement* (previously cited); iLaw, *Parasite That Smiles: Pegasus Spyware Targeting Dissidents in Thailand* (previously cited).

[70] UN Special Rapporteurs, Letter to the Thai government on the use of Pegasus spyware, 19 April 2023, UN Doc. AL THA 1/2023, https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=27942

[71] UN Special Rapporteurs, Letter to the Thai government on the use of Pegasus spyware (previously cited). While the initial The Citizen Lab and Digital Reach, provided a list of 30 individuals whose devices were infected with Pegasus spyware, subsequent research increased this number to 35. See footnote 1 for more details.

39. In 2024, Amnesty International built upon the research on Pegasus spyware in Thailand through interviews with women activists in Thailand who had been targeted, as part of a report on the impacts of tech-facilitated gender-based violence. The report outlined how the use of Pegasus against HRDs infringed on their human rights, including the rights to freedom of expression, peaceful assembly and association, the right to an effective remedy, and constituted unlawful interference with privacy.[72] NSO Group has not publicly disclosed any information regarding investigation into the cases of Pegasus use against individuals in Thailand, including against the Plaintiff, in response to any of the published research.

40. It is important to note that the secrecy surrounding the spyware trade and use is such that independent forensic analysis cannot unequivocally attribute the known cases of targeted digital surveillance using Pegasus against HRDs to specific Thai or other state actors. However, the weight of technical and circumstantial evidence leads Amnesty International to conclude that there is a strong likelihood that one or more Thai state actors, or agents acting on their behalf, were involved in the use of the spyware. This is especially so because NSO Group has consistently declared that NSO products are sold only to government intelligence and law enforcement agencies[73]. NSO Group has not publicly disclosed any information on the due diligence processes carried in relation to the sale, nor any efforts to monitor the use of Pegasus, in Thailand. Amnesty International sent a letter on 5 April 2024 to NSO Group and other related legal entities to inquire the companies about the criteria and protocols followed to carry out due diligence for evaluating adverse human rights impacts in Thailand. However, NSO Group has not replied to this letter.

NSO has a responsibility to conduct HRDD by effectively monitoring the use of Pegasus to identify, prevent, mitigate, and account for adverse human rights impacts.

41. As outlined in the previous section, NSO Group have a duty to exercise due diligence to identify, prevent, mitigate and account for any adverse human rights impacts they cause, contribute to, or are directly linked to their operations, products, or services. Therefore, NSO Group should carry out HRDD assessments of their entire value chain before entering into and throughout the contractual relationship with clients and users of its product, and take appropriate action based on the findings of such assessments. If the company had conducted such due diligence, and had sold the Pegasus spyware to Thai authorities, then NSO Group should have been aware of the history of digital repression against human rights activists and peaceful protesters in Thailand. With such constructive knowledge, it would have had to be aware when it sold Pegasus spyware, including the sale that led to the violations described above (even if it did so through a distributor), that this product could or would cause direct human rights harms.

42. While NSO Group states that it does not control the tool known as Pegasus, it appears that Pegasus is at least directly linked to human rights abuses committed by certain clients, including those who harmed Mr. Jatupat Boonpattararaksa. While the requirements of the UN Guiding Principles relating to remediation are confined to cases where business enterprises have caused or contributed to adverse impacts, this does not imply that companies can ignore impacts that may be directly linked to their operations, products or services. NSO Group has a responsibility to use its leverage with those clients to prevent and mitigate harm to human rights.[74] NSO Group can do so by ceasing the use, production, sale, transfer and support of Pegasus spyware to those clients until the company develops technical safeguards that can ensure its lawful use.[75] It should also provide adequate compensation or other forms of effective redress where the company identifies it has contributed to harm to survivors of unlawful surveillance.

Thai courts must protect individuals under its jurisdiction from human rights abuses, including by guaranteeing the

[72] Amnesty International, *"Being ourselves is too dangerous": Digital violence and the silencing of women and LGBTI activists in Thailand*, 16 May 2024, ASA 39/7955/2024, https://www.amnesty.org/en/documents/asa39/7955/2024/en/

[73] NSO Group, "About Us" (previously cited), (accessed on 27 August 2024).

[74] OHCHR, UN Guiding Principles on Business and Human Rights (previously cited), Commentary to Principle 19 Commentary.

[75] Pegasus spyware does not currently include technical safeguards to ensure that the highly invasive spyware does not cause human rights harm as it is specifically designed to evade investigation and allows for its users to take the maximum amount of target data possible.

right to privacy and the right to an effective remedy.

43. The fifth submission by the Intervener is that the claim should be able to proceed in Thailand courts, since, under IHRL, Thailand has an obligation to prevent and protect against human rights violations and abuses, including the violation of the right to privacy as a result of Pegasus spyware. To address the violations of various human rights outlined above, the Thai government has the obligation to guarantee an effective remedy and reparations for individuals subjected to human rights abuses, such as facing a violation of their right to privacy, as reflected in the third pillar of the UN Guiding Principles.[76] Principle 26 also reinforces the duty of States to "take appropriate steps to ensure the effectiveness of domestic judicial remedies" including by "reduc[ing] legal, practical and other relevant barriers that could lead to a denial of access to remedy."[77] In discharging this obligation, the Intervener respectfully notes to the Court that, as addressed above, the UN Guiding Principles provide that when business enterprises identify they have caused or contributed to human rights harm they should provide for or cooperate in their remediation through legitimate processes.

V. CONCLUSION

44. Amnesty International respectfully submits that to ensure good-faith adherence to Thailand's international human rights obligations, Thai law must be interpreted so as to ensure conformity with IHRL. The Intervener invite the Court to conclude that the Defendant owed the Plaintiff a responsibility to conduct Human Rights Due Diligence by effectively monitoring the use of Pegasus to identify, prevent, mitigate, and account for adverse human rights impacts, including those to which Pegasus is directly linked by the Defendant's business relationship with certain clients that caused harm to the Plaintiff. Moreover, Amnesty International respectfully invites the Court to determine whether the Defendant's responsibility under IHRL and standards has a bearing on their alleged liability and, if so, issue an appropriate judgment to ensure the right to an effective remedy and reparation for the plaintiff as a survivor of unlawful surveillance that violated his human rights.

---

[76] OHCHR, UN Guiding Principles on Business and Human Rights (previously cited), Pillar III, Principle 25, including Commentary.

[77] OHCHR, UN Guiding Principles on Business and Human Rights (previously cited), Principle 26, including Commentary.