IN THE SUPREME COURT OF INDIA

CIVIL ORIGINAL JURISDICTION

WRIT PETITION (CIVIL) NO. 849 OF 2021

IN THE MATTER OF: -

JAGDEEP S. CHHOKAR ...PETITIONER

VERSUS

UNION OF INDIA ...RESPONDENT

AFFIDAVIT OF PROFESSOR DAVID KAYE AND THE INTERNATIONAL JUSTICE CLINIC OF THE UNIVERSITY OF CALIFORNIA, IRVINE, SCHOOL OF LAW

I, David Kaye, S/o Dr. Jerry H. Kaye, aged about 53 years, resident of Los Angeles, California, United States of America do hereby solemnly affirm:

1. I am an expert in the field of international human rights law. My academic and professional background makes me and the Clinic that assisted in the preparation of this affidavit well-suited to introduce to this Court the depth and scope of the right to freedom of expression under international human rights law. I am including as annex with this submission a recent curriculum vitae marked as "**Annexure 1.**"
2. From 2014 to 2020, I served as the United Nations ("UN") Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. In that role —with the support of the International Justice Clinic at the University of California, Irvine, School of Law—through detailed research and official country missions, I monitored trends concerning the freedoms of opinion and of expression globally and reported on those trends to the UN General Assembly and

Human Rights Council. My reporting to the UN addressed, among other subjects, the impact of technology on the enjoyment of human rights, encryption and anonymity, the protection of whistleblowers and journalistic sources, the surveillance industry, the human rights obligations of governments, and responsibilities of companies in the Information and Communications Technology sector, the regulation of online content by social media and search companies, Artificial Intelligence technologies and human rights, and online hate speech. Of special relevance to the cases before this Court, in May 2019, I submitted a report to the UN Human Rights Council regarding the private surveillance industry, which I am including as annex with this submission marked as "**Annexure 2.**"

3. Since 2012, I have been serving as a Clinical Professor of Law at the University of California, Irvine, School of Law, and Director of the Law School's International Justice Clinic. My teaching and research have focused on international human rights law, technology and international law, and other subjects in public international law. As an expert in the field of international human rights law, I have published a book on technology and human rights, as well as numerous law review articles, book chapters, and opinion essays on the topic.
4. This intervention seeks to provide the Court with information concerning the rights individuals enjoy under international human rights law, especially in the context of surveillance technologies and in particular under the International Covenant on Civil and Political Rights ("ICCPR" or "Covenant").

I. SURVEILLANCE INTERFERES WITH SEVERAL RIGHTS UNDER THE COVENANT, ESPECIALLY RIGHTS TO

PRIVACY AND FREEDOM OF OPINION AND EXPRESSION

5. We live in an age when digital surveillance is readily available, easy to abuse, and difficult to detect.[1] Surveillance casts a shadow over different forms of expression such that individuals are intimidated into refraining from, or harassed or held criminally liable for, activities protected under international human rights law.[2] In particular, digital surveillance interferes with the right to privacy in a way that has significant implications for the exercise of the rights to freedom of opinion and expression. Additionally, mass and targeted surveillance programs operate in such ways that they are often unknown to those whose activities have been collected and observed, creating a perverse sense of violation – with the related consequences of limiting fully legitimate expression – even when the specific acts of surveillance are difficult, if not impossible, to determine. The UN High Commissioner for Human Rights, in a landmark report on privacy in digital contexts in 2014, stated that international human rights law provides a clear and universal framework for the protection of the right to privacy, including in the context of domestic and extraterritorial surveillance, and concluded that practices in many States involved a lack of adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight, all of which have contributed to a lack of accountability for unlawful digital surveillance.[3]

6. While holding the mandate of the UN Special Rapporteur, I authored a report regarding freedom of expression in the era of online surveillance,

---

[1] *See Report of the UN special Rapporteur on surveillance and human rights*, A/HRC/41/35 (May 28, 2019), ¶ 24 [hereinafter *2019 Report on surveillance*].

[2] OHCHR, Report of the Office of the United Nations High Commissioner for Human Rights, *The right to privacy in the digital age* (30 June 2014) A/HRC/27/37, ¶ 47 [hereinafter *Report on the right to privacy in the digital age*]; *Report of the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue on Surveillance* (17 April 2013) A/HRC/23/40, ¶79 [hereinafter *2013 Report on surveillance*].

[3] *Report on the right to privacy in the digital age*, ¶47.

in which I expressed deep concern regarding technologies that facilitate targeted surveillance.[4] In the report, I examined the wide range of private surveillance tools and how their use conflicts with human rights law, specifically how it impacts the rights to privacy, freedom of opinion and expression, freedom of association, and freedom from discrimination, among others:

> "Targets of surveillance suffer interference with their rights to privacy and freedom of opinion and expression whether the effort to monitor is successful or not. The target need have no knowledge of the attempted or successful intrusion for the interference with their right to privacy to be complete. Indeed, Governments generally seek tools that intrude without the knowledge of the target. However, it is critical to see such interference as part of an overall effort to impose consequences on the target. If conducted for unlawful purposes, the attempt at surveillance – and the successful operation – may be used in an effort to silence dissent, sanction criticism or punish independent reporting (and sources for that reporting)."[5]

7. Not all surveillance operations constitute a violation of human rights law; some restrictions may meet the conditions of legality, legitimacy, and proportionality. However, because of the risks they involve to fundamental rights, all types of surveillance practices call for a rigorous evaluation of whether they are consistent with norms of international human rights law.

A. International Law Guarantees and Protects the Right to Privacy

8. Article 17 of the Covenant – which India ratified in 1979 – guarantees the

[4] *See 2019 Report on surveillance*.
[5] *Id.*, ¶21.

right to privacy and freedom from arbitrary or unlawful interference.[6] Article 17 also creates an affirmative state obligation to protect individuals from attacks on one's privacy.[7] This includes an obligation for States not to intrude on privacy themselves and the corollary obligation to protect individuals from third-party intrusions.

9. Article 17(2) of the Covenant provides that "[e]veryone has the right to the protection of the law against such interference or attacks" and Article 2 imposes duties on States to uphold that specific right. An interference into an individual's right to privacy is therefore only permitted under article 17 if conducted in such a manner that is neither arbitrary or unlawful.[8] The UN High Commissioner for Human Rights has stated that global standards require that any restriction on the right to privacy must meet the tests of legality, necessity and proportionality.[9] In 2017 the Human Rights Council reaffirmed this standard in its Resolution 34/7 on the right to privacy in the digital age by recalling that "States should ensure that any interference with the right to privacy is consistent with the principles of legality, necessity and proportionality."[10] Article 17 of the Covenant permits interferences with the right to privacy only in circumstances that are "authorized by domestic law that is accessible and precise and that conforms to the requirements of the Covenant," are in pursuit of "a legitimate aim," and that satisfy the requirements of "necessity and proportionality."[11] This test for permissible interference in

---

[6] International Covenant on Civil and Political Rights art. 17, Dec16, 1966, 999 U.N.T.S. 171.
[7] UN Human Rights Committee, General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, (8 April 1988).
[8] *Report on the right to privacy in the digital age*, ¶21.
[9] *Report on the right to privacy in the digital age*, ¶21-23.
[10] Huma Rights Council, Resolution 34/7 The right to privacy in the digital age (27 March 2017) UN.doc. A/HRC/RES/34, ¶2.
[11] Human Rights Committee, General Comment No. 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant (29 March 2004) UN doc. HRI/GEN/1/Rev.9, ¶6; *Report on the right to privacy in the digital age*, ¶ 23. *See also, Report of the Special Rapporteur on the promotion and protection of human rights while countering terrorism on the use of mass digital surveillance for counter-terrorism*, A/69/397 (23 September 2014), ¶30 [hereinafter "*Report on the use of mass digital surveillance for counter-terrorism"*].

the context of surveillance that burdens speech works in tandem with the applicable standards governing restrictions on freedom of expression under Article 19(3) of the Covenant, outlined below.

10. Targeted surveillance that, like the spyware at issue in this proceeding, covertly accesses information on an individual's phone threatens the right to privacy. The UN General Assembly has stated that privacy is fundamental to the realization of the freedom of opinion and expression as it provides the conditions for these key rights.[12] Absent an expectation of privacy, the ability for individuals to form a diversity of opinions and for them to seek and impart information and ideas of all kinds is compromised. Targeted surveillance—or even the mere possibility of it—creates an interference with privacy, with a potential chilling or inhibiting effect on the exercise if the rights to freedom of expression and association.[13] It "creates incentives for self-censorship and directly undermines the ability of journalists and human rights defenders to conduct investigations and build and maintain relationships with sources of information."[14] In environments where the targeted communities know of or suspect attempts at illicit surveillance, such awareness itself "shapes and restricts their capacity to exercise the rights to freedom of expression [and] association"[15] among others. This is because the attempt at surveillance and its successful operation are likely to be used "in an effort to silence dissent, sanction criticism or punish independent reporting (and sources for that reporting). The sanctions may not only apply to the targets but to their networks of contacts as well."[16] In short, interference

[12] UN General Assembly, A/RES/68/167 (Dec. 18. 2014).
[13] See *Report on the right to privacy in the digital age*, ¶ 20; Human Rights Committee, General Comment No. 37 on the right of peaceful assembly (article 21), CCPR/C/GC/37 (17 September 2020) ¶70-71 [hereinafter "General Comment 37];*Report of the UN Special Rapporteur on the rights to freedom of peaceful assembly and of association on the rights to freedom of peaceful assembly and of association in the digital age*, A/HRC/41/41 (May 17, 2019), ¶ 50-57 [hereinafter *Report on assembly and association in the digital age*].
[14] *2019 Report on surveillance*, ¶ 26.
[15] *2019 Report on surveillance*, ¶ 21.
[16] *2019 Report on surveillance*, ¶ 21.

with privacy through targeted surveillance typically represses the exercise of the right to freedom of expression.

11. Privacy protection technologies like encryption and anonymity can help establish forums to protect the freedoms of opinion and expression as they ordinarily ensure that only intended recipients of communications receive them.[17] However, targeted surveillance gives users access to these communications by exploiting vulnerabilities in encryption and anonymity technology, making it impossible for targeted individuals to protect their privacy.
12. In a contemporary era in which digital communications and activities constitute a significant share of all human activities, privacy is essential in protecting and securing freedom of opinion and expression.[18]

B. International Law Protects Freedom of Opinion and Expression

13. The ICCPR, like the Universal Declaration of Human Rights before it, protects the right to seek, receive, and impart information and ideas of all kinds through any media and regardless of frontiers. The Human Rights Council, the central human rights body of the UN system and a subsidiary body of the UN General Assembly, has proclaimed freedom of expression to be one of the essential foundations of a democratic society and a condition for its progress and development.[19] Among other things, freedom of opinion and expression is essential in the conduct of public affairs and the effective exercise of the right to vote, which necessitates free flow of ideas and communications about political issues.
14. Article 19(1) of the ICCPR prohibits *any* restriction on the freedom of

---

[17]*Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on encryption and anonymity*, A/HRC/29/32 (May 22, 2015), ¶ 17 [hereinafter *Report on encryption and anonymity*].
[18]*See* David Kaye, *Amicus Curiae in the Case of Privacy International and Others v. the United Kingdom*(2019) https://freedex.org/wp-content/blogs.dir/2015/files/2019/10/Amicus_PI-v-UK_Intervention.pdf
[19]Human Rights Council, A/HRC/RES/21/12 (Oct. 9, 2012); Human Rights Council, A/HRC/23/L.5 (April 9, 2014), ¶ 2.

opinion.[20] The freedom of opinion protects all forms of opinions from impairment and interference. Actual, perceived, or supposed opinions are protected equally.[21] Impairment means harassment, surveillance[22], stigmatization, or any act of coercion which would interfere with the presence of an opinion or lack thereof.[23]

15. Spyware has the potential to interfere with the freedom of opinion. While encryption and anonymity technologies ordinarily maintain a zone of privacy where opinions may be freely held and shared amongst individuals, spyware accesses an individual's opinions without consent or, often, legal authority, undermining the security provided by encryption or anonymity tools. By remaining anonymous, individuals can seek, receive and impart ideas and opinions that may be unavailable to them otherwise, particularly in repressive or censorship-driven environments. Encryption may ensure that only intended recipients have access to messages, information, or data. However, the use of spyware transgresses both anonymity and encryption, thus threatening the ability of individuals to form and hold opinions without any interference.[24] Individuals without the privacy protections afforded by encryption and anonymity may be deterred from viewing and searching for information out of a fear that their activities may be disclosed through surveillance activities without their consent or knowledge.
16. Article 19(2) of the Covenant articulates a robust freedom of expression, requiring that governments protect and ensure the right to seek, receive and impart information and ideas of all kinds, regardless of frontiers and

---

[20] ICCPR, art. 19.
[21] Human Rights Committee, General Comment No. 34 on the right to freedom of expression, CCPR/C/GC/34, (12 September 2011) ¶ 9[hereinafter "General Comment 34"].
[22] *Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on encryption and anonymity*, A/HRC/29/32(May 22, 2015), ¶ 6 [hereinafter *Report on encryption and anonymity*].
[23] General Comment 34, ¶ 9.
[24] *Report on encryption and anonymity*, ¶ 21.

through any media. The Human Rights Committee, as the principal monitor and interpreter of the ICCPR, has emphasized the centrality of Article 19 to democratic governance by underlining that the freedom of expression is "a necessary condition for the realization of the principles of transparency and accountability that are, in turn, essential for the promotion and protection of human rights."[25]

17. Article 19(3) of the ICCPR allows for narrow restrictions on the freedom of expression (but not on the freedom of opinion). Pursuant to that provision, any restriction, to be legitimate, must be provided by law and necessary in order to achieve one of the legitimate objectives discussed below. A government imposing a burden on expression must demonstrate that the restrictions meet the tests of legality, legitimacy, and necessity.

18. The legality test requires that a public authority demonstrate that any restriction of freedom of expression is provided by law in a manner that is precise, public, and transparent. All laws restricting expression must be clear, accessible, predictable, and detailed enough to give individuals appropriate notice as to what constitutes restricted expression and so they may regulate their conduct accordingly.[26] Legislation must specify that State surveillance may only be used under "the most exceptional circumstances and exclusively under the supervision of an independent judicial authority. Safeguards must be articulated in law relating to the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided by the national law."[27] Additionally, individuals should have "a legal right to be notified that they have been subjected to communications surveillance or that their

[25] General Comment 34, ¶ 9.
[26] Human Rights Committee, *Korneenko et al. v. Belarus*, *Communication No. 1553/2007;* General Comment 34, ¶
25.
[27] *2013 Report on surveillance*, ¶81.

communications data has been accessed by the State."[28] Considering that such notification might jeopardize the effectiveness of legitimate uses of surveillance, individuals "should nevertheless be notified once surveillance has been completed and have the possibility to seek redress in respect of the use of communications surveillance measures in their aftermath."[29]

19. The legitimacy test requires a public authority to demonstrate that any limitation addresses one of the permissible interests specified by Article 19(3). Permissible interests include respecting the rights or reputations of others, or for the protection of national security or of public order (*ordre public*), or of public health or morals.[30] However, the restriction cannot be such that it would render the right itself meaningless.[31] Restrictions on rights must be an exception, not the norm. It is important to highlight that "national security" – much as the Court described in its October 27th decision – cannot be used as a blanket justification for every interference with human rights. States regularly invoke national security to legitimize surveillance measures that entail overbroad restrictions on human rights.[32] The invocation of national security does not in and of itself provide an adequate human rights law justification.[33] Rather, the State must provide an "articulable and evidence-based justification for the interference."[34] The State must, at a minimum, give a meaningful public account of the tangible benefits of a restriction.[35]

20. The third condition requires that the relevant public authority

[28] *2013 Report on surveillance*, ¶82.
[29] *2013 Report on surveillance*, ¶82.
[30] ICCPR, art. 19.
[31] General Comment 34, ¶ 21.
[32] *2013 Report on surveillance*, ¶ 59 – 60.
[33] *Report on the use of mass digital surveillance for counter-terrorism*, ¶ 11*; Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression on Freedom of Expression and the Internet and Telecommunications Access Industry*, A/HRC/35/22 (March 30,2017), ¶ 18.
[34] *Report on the use of mass digital surveillance for counter-terrorism*, ¶ 12.
[35] *Id*. ¶ 14.

demonstrate the necessity and proportionality of any restriction. In other words, a State must demonstrate that said restriction is necessary to protect one of the enumerated legitimate interests and that the restriction is the least restrictive means of achieving that legitimate interest.[36]Any restriction must have a direct and immediate connection between the expression and the threat.[37] Because targeted surveillance often collects or monitors *all* data on an individual's phone, the use of targeted surveillance must pass a very high bar to meet the necessity and proportionality requirement.

21. Restrictions on freedom of expression must not only comply with the strict requirements previously mentioned, but "must also themselves be compatible with the provisions, aims and objectives of the [ICCPR]. Restrictions must not violate the non-discrimination provisions of the Covenant."[38]

C. International Law Protects Freedom of Association and Assembly

22. Article 21 of the ICCPR protects the right to assemble peacefully "wherever they take place: outdoors, indoors and online; in public and private spaces; or a combination thereof".[39] Article 22 of the Covenant protects the right to freedom of association. As with all ICCPR rights, the freedom of association and assembly are rights that must be provided without discrimination.[40] States have both a negative obligation to abstain from interfering with the right to peaceful assembly and a positive obligation to facilitate and protect these rights.[41] No restrictions may be placed unless they are necessary in a democratic society in the interests of national security or public safety, public order (*ordre public*), the

[36] *2019 Report on surveillance*, ¶ 24
[37] *Id*. at ¶ 8.
[38] General Comment 34, ¶ 26.
[39] General Comment 37, ¶ 6.
[40] *Report on assembly and association in the digital age*, ¶ 13.
[41] *Report on assembly and association in the digital age*, ¶ 13.

protection of public health or morals or the protection of the rights and freedoms of others.[42] Thus, similarly to freedom of expression, freedom of association and assembly can be limited only if the requirements of legality, legitimacy, and necessity are met.

23. Targeted surveillance may result in an interference with the freedom of peaceful assembly and association. These rights may be exercised and are protected equally online as well as offline. States recently have been utilizing surveillance against civil society actors who plan to stage peaceful public assemblies.[43] The right to peacefully assemble online includes the right to remain anonymous unless there are reasonable grounds for arrest or other compelling reasons.[44] Targeted surveillance has the potential to strip individual participants of this right indiscriminately, without a State agent first having reasonable grounds for doing so. As spyware capabilities become increasingly more sophisticated, the potential for its abuse to prevent the formation or staging of peaceful assemblies also is increasing.

II. PRIVATE SURVEILLANCE MALWARE LIKE NSO GROUP'S PEGASUS RISK SERIOUS INTERFERENCE WITH THE RIGHTS TO PRIVACY AND FREEDOM OF OPINION AND EXPRESSION

24. Pegasus, the spyware developed by the Israeli Company NSO Group, is considered to be one of the most powerful and sophisticated surveillance tools ever created.[45] Pegasus allows its deployers to hack directly into an individuals' mobile devices, access all of the information on those devices, and control access to the devices' camera and recording

[42] ICCPR, art. 21.
[43] *Report on assembly and association in the digital age*, ¶ 29.
[44] General Comment 37, ¶ 60.
[45] David Pegg and Sam Cutler, *What is Pegasus spyware and how does it hack phones?* The Guardian (18 July 2021) https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones

functions. Citizen Lab, a Canadian university research organization, has identified Pegasus software being used as a surveillance tool targeting individuals in more than 50 countries, including India, Saudi Arabia, and the United States.[46] Amnesty International, a UK based human rights non-governmental organization, supported the international consortium of journalists under the umbrella of Forbidden Story's "Pegasus Project", which has shown that Pegasus is being used by states to silence journalists, activists, and political dissenters around the globe.[47]

25. The NSO Group has repeatedly stated that it sells Pegasus exclusively to governmental agencies to help them fight terrorism, drug and sex trafficking, and other serious crimes.[48] However, many reports from various countries indicate that governments have used Pegasus software against journalists, scholars, and political dissidents. A leaked list of more than 50,000 phone numbers indicates that Pegasus malware may have been used to infect the mobile devices of many political and public figures, including a Dubai princess,[49] French President Emmanuel Macron,[50] and the fiancée of the late Saudi journalist Jamal Khashoggi.[51]

---

[46]Forbidden Stories, *About the Pegasus Project* (2021), https://forbiddenstories.org/about-the-pegasus-project/; Bill Marczak, et. al., *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, Citizen Lab (18 September 2018) https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45- countries/

[47]Amnesty International, *Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally* (18 July 2021) https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/

[48] NSO Group, *Following the publication of the recent article by Forbidden Stories, we wanted to directly address the false accusations and misleading allegations presented there* (2021)https://www.nsogroup.com/Newses/following-the-publication-of-the-recent-article-by-forbidden-stories-we-wanted-to-directly-address-the-false-accusations-and-misleading-allegations-presented-there/

[49] Drew Harwell, *Dubai ruler used Pegasus spyware to hack princess's phone, U.K. court rules*, Washington Post (6 October 2021) https://www.washingtonpost.com/technology/2021/10/06/pegasus-dubai-princess-haya-court-ruling/

[50] Angelique Chrisafis, Dan Sabbagh, Stephanie Kirchgaessner and Michael Safi, *Emmanuel Macron identified in leaked Pegasus project data* (20 July 2021) https://www.theguardian.com/world/2021/jul/20/emmanuel-macron-identified-in-leaked-pegasus-project-data

[51]Dana Priest, Souad Mekhennet and Arthur Bouvart, *Jamal Khashoggi's wife targeted with spyware before his death* (18 July 2021) https://www.washingtonpost.com/investigations/interactive/2021/jamal-khashoggi-wife-fiancee-cellphone-hack/ ; Amnesty International, *Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally* (18 July 2021) https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/

26. The intrusive nature of Pegasus technology poses questions about whether it can ever be used in a way that is consistent with international human rights law. While not the only spyware software on the market, due to the power of Pegasus, technology and human rights experts have supported a ban or at least a moratorium on the development, transfer and use of intrusive spyware in order to ensure that human rights may be adequately protected.[52] In the absence of a ban, spyware tools need to be subject to strict regulations in order to be as consistent with international human rights law. The following subsections will address these two arguments.

A. Incompatibility of private surveillance software like Pegasus with international human rights standards

27. Once individuals are under suspicion and subject to formal investigation by law enforcement or intelligence agencies, there may be circumstances according to which they may be subjected to surveillance for legitimate counter-terrorism and law enforcement purposes when constrained by fundamental rule of law standards.[53] As previously mentioned, it is understood that both articles 17 and 19 of the ICCPR allow for narrow limitations on the right to privacy and freedom of expression provided that (i) they are authorized by law that is accessible and precise and that conforms to the requirements of the Covenant, (ii) they pursue a legitimate aim and (iii) they meet the tests of necessity and proportionality. The question posed by spyware like Pegasus is whether it

---

[52] *2019 Report on surveillance*, ¶2; *see* David Pegg and Paul Lewis, *Edward Snowden calls for spyware trade ban amid Pegasus revelations*, The Guardian (19 July 2021) https://www.theguardian.com/news/2021/jul/19/edward-snowden-calls-spyware-trade-ban-pegasus-revelations; Irene Khan, Special Rapporteur on the promotion and protection of the right to freedom of expression, et.al, *Spyware scandal: UN experts call for moratorium on sale of 'life threatening' surveillance tech* (12 August 2021)*https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27379&LangID=E*

[53] *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism on the right to privacy in the fight against terrorism*, A/HRC/13/37 (28 December 2009), ¶ 13

can ever – given its intrusive nature – comply with this three-part test.

28. First, with regards to the legitimacy of the restriction, while the prevention of terrorism is a legitimate aim for this purpose, "the activities of intelligence and law enforcement agencies in this field must still comply with international human rights law."[54] NSO Group maintains that it sells Pegasus to help governments fight terrorism and solve crimes,[55] and yet reporting by Citizen Lab, Amnesty International, *The Guardian*, *The Washington Post*, and other organizations indicates that many victims of Pegasus malware have been journalists and political activists.[56] For instance, according to an Amnesty International report, Mexican journalist Cecilio Pineda's phone was selected for spyware targeting just weeks before his killing in 2017.[57] While it is not clear whether the targeting of Pineda's phone contributed to his death, the possibility of targeted—thus discriminatory—use of surveillance technology raises a question of a potential human rights violation on discrimination grounds. Most recently, it was revealed that phone numbers of Palestinian rights advocates who work in West Bank were infected with Pegasus.[58]

29. These examples suggest that Pegasus is used to surveil and silence activists, opposition leaders, and journalists. There is evidence in the cited documents that Pegasus is used for targeted surveillance of individuals who belong to cognizable social groups (e.g. journalists, human rights defenders, and others who belong to racial, religious,

---

[54] *Report on the use of mass digital surveillance for counter-terrorism*, ¶ 12.
[55] NSO Group, About Us, https://www.nsogroup.com/about-us/
[56] Amnesty International, *Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally* (18 July 2021) https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/
[57] Amnesty International, *Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally* (18 July 2021), https://www.amnesty.org/en/latest/news/2021/07/the-pegasus-project-2/
[58] Amnesty International, *Devices of Palestinian Human Rights Defenders Hacked with NSO Group's Pegasus Spyware* (8 November 2021) https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-human-rights-defenders-hacked-with-nso-groups-pegasus-spyware-2/

ethnic, national or other minority communities); such use is discriminatory in nature and raises concerns under the Covenant's Article 2 prohibition of such discrimination. As referenced above, any limitation of a fundamental human right, including a right to privacy and freedom of expression, must pass the legitimacy test. State uses of Pegasus to target journalists, community leaders, and regime critics do not meet the legitimacy test and are inconsistent with international law.

30. Second, the use of surveillance technologies such as the Pegasus software effectively annuls the right to privacy of communications altogether. By permitting indiscriminate access to all digital communications and data, this technology eliminates the possibility of any necessity or proportionality analysis. That is, a State must demonstrate that a restriction is necessary to protect one of the legitimate interests, that there is a rational connection between the means used and the aim sought to be achieved, and that the restriction is the least restrictive means of achieving that legitimate interest.[59] A proportionality analysis requires assessing a state's assertion that the extent of the intrusion into the right achieves the specific benefit of carrying out the investigations undertaken by a public authority in the public interest.[60]

31. Pegasus is a tool that was created with a specific goal in mind—to allow actors access to private conversations, images, and data stored on the mobile devices of others. An actor that hacks into a mobile device of another person using Pegasus can access all the conversations, activate video and audio recordings, and delete and download all digital data, including but not limited to information about third parties and minors as well as information that falls outside the scope of inquiry.[61]

---

[59] General Comment 34, ¶ 33.
[60] *Report on the use of mass digital surveillance for counter-terrorism*, ¶ 51.
[61] David Pegg and Sam Cutler, *What is Pegasus spyware and how does it hack phones?* The Guardian (18 July 2021) https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones

32. Because Pegasus gives actors unrestrained access to personal data of others, its use may generally violate the proportionality requirement, regardless of whether a State invokes one of the legitimate aims. Restriction of freedom of expression and privacy must be *narrowly* tailored and have a direct and *immediate connection* between the means used and the aim it seeks to achieve. As the UN Special Rapporteur on human rights and counter-terrorism has noted, "The fact that something is technically feasible, and that it may sometimes yield useful intelligence, does not by itself mean that it is either reasonable or lawful."[62]
33. The intrusiveness of Pegasus spyware requires, at a minimum, that governments deploying it demonstrate that its use constitutes the least intrusive way of achieving a legitimate objective. Moreover, Pegasus has been seen to deploy zero-click infections, such that device owners need not do anything to become infected other than receive a message or other communication.[63] The delayed detectability of zero-click entries also delays the time by which serious misuses may be prevented. This problem is not just a hypothetical, it has already been demonstrated. An Apple iMessage vulnerability was taken advantage of by the use of Pegasus. On September 7, 2021, Citizen Lab informed Apple about the vulnerability and on September 13th Apple confirmed that the files sent by the organization included a zero-day exploit against iOS and MacOS and subsequently released an update to patch the vulnerability.[64]
34. As the Human Rights Committee has emphasized, "in no case may the restrictions be applied or invoked in a manner that would impair the

[62] *Report on the use of mass digital surveillance for counter-terrorism*, ¶11.
[63] Bill Marczak, *FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild*, CitizenLab (13 September 2021) https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/
[64] *Id*; Zack Whittaker, *Apple patches an NSO zero-day flaw affecting all devices*, Tech Crunch (13 September 2021) https://techcrunch.com/2021/09/13/apple-zero-day-nso-pegasus/

essence of a Covenant right."[65]Whether a government publicly admits to buying and using Pegasus or the public suspects that such a tool may be used against them, it leads to a chilling or inhibiting effect on human rights.[66] The chilling effect implies that people no longer enjoy their freedom of opinion, expressions, assembly, and many others, because they fear invasion of privacy or arbitrary persecution.

35. In conclusion, given the nature of this tool and its indiscriminate and pervasive capabilities, spyware like Pegasus deserves the most robust scrutiny in order to determine whether its use is compliant with human rights law.

B. Spyware tools need to be subject to strict regulations in order to be consistent with international human rights law

36. Given the extraordinary risk of abuse of these surveillance tools, and in the absence of a ban on their use, States should have in place strict regulations in accordance with international human rights law.

37. Regulation authorizing the use of surveillance tools must be "narrowly and precisely formulated" so as to enable those affected by such laws to foresee what powers may be used against them,[67] and to minimize the risk of excessive discretion on part of the government authorities in terms of interpreting the provisions.[68] The laws should be publicly accessible and must provide for effective safeguards against abuse. Particularly, the use of surveillance must be subject to authorization by an independent and impartial judicial body with all appropriate limitations on time, manner, place and scope of the surveillance.[69] Additionally, there should

[65]Human Rights Committee, General Comment No. 27 on the right to freedom of movement, CCPR/C/21/Rev.1/Add.9 (2 November 1999); General Comment 31.
[66]*2013 Report on surveillance*, ¶ 52
[67]*Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin*, A/HRC/14/46, ¶ 10-11 (May 17, 2010).
[68]*Report on the right to privacy in the digital age*, ¶ 29.
[69]*2019 Report on surveillance*, ¶ 50.

be an adjudicatory body responsible for oversight with competence to make judicial decisions about the legality of surveillance, the technologies used and human rights involved, and have adequate resources in exercising their functions.[70] Also, individuals "should have a legal right to be notified that they have been subjected to communications surveillance."[71] When such notification jeopardizes the effectiveness of investigations, individuals should "should nevertheless be notified once surveillance has been completed and have the possibility to seek redress in respect of the use of communications surveillance measures in their aftermath."[72] The purchase and use of these types of surveillance software "should also be subject to meaningful public oversight, consultation and control."[73]

38. Further, the State should publish information of the scope of communications surveillance techniques and powers to provide "individuals with sufficient information to enable them to fully comprehend the scope, nature, and application of the laws permitting communications surveillance."[74] The Indian Supreme Court's decision of October 27, 2021 to establish a three-member technical expert committee, is a step forward into this regard. One of the Committee's central goals is to shed light on whether Pegasus was used on Indian citizens and if so, how it was done. The Committee will investigate and determine the details of those affected, the steps taken by the government once the information regarding the use of Pegasus against Indian citizens was made public, whether any "Pegasus suite of spyware was acquired by the Respondent Union of India, or any State Government, or any central or

[70] Electronic Frontier Foundation, *International Principles on the Application of Human Rights to Communications Surveillance* (10 July 213) https://www.eff.org/files/necessaryandproportionatefinal.pdf.
[71] *2013 Report on surveillance*, ¶ 82.
[72] *2013 Report on surveillance*, ¶ 82.
[73] *2019 Report on surveillance*, ¶ 52.
[74] *2013 Report on surveillance*, ¶ 92.

state agency [or by any domestic entity/person] for use against the citizens of India" and if so, under what "law, rule, guideline, protocol or lawful procedure was such deployment made." This Committee is especially valuable due to the government's reluctance to "clarify its stand regarding the allegations raised, and to provide information to assist the Court regarding the various actions taken by it over the past two years, since the first disclosed alleged Pegasus spyware attack."[75]

III. CONCLUSION

39. The freedoms guaranteed by international human rights law are threatened by any government's secretive purchase and use of Pegasus software. A failure to disclose the purchase and use of Pegasus interferes with the public's freedom of opinion, expression, and privacy. States are increasingly recognizing the danger posed by technologies like Pegasus. In November of 2021, the US Department of Commerce blacklisted the NSO Group and stated that the current administration is committed to putting "human rights at the center of U.S. foreign policy."[76] This is a powerful statement of the US Government about the incompatibility of Pegasus spyware with the human rights framework and digital privacy and security.[77]
40. The use of Pegasus against individuals risks consistent and regular disproportionality given its vast powers to sweep in everything associated

[75] Supreme Court of India, Writ Petition (Crl.) No. 314 of 2021 *Manohar Lal Sharma v. Union of India and Ors with* Writ Petition (Civil) No. 826 Of 2021, Writ Petition (Civil) No. 909 Of 2021, Writ Petition (Civil) No. 861 Of 2021, Writ Petition (Civil) No. 849 Of 2021, Writ Petition (Civil) No. 855 Of 2021, Writ Petition (Civil) No. 829 Of 2021, Writ Petition (Civil) No. 850 Of 2021, Writ Petition (Civil) No. 848 Of 2021, Writ Petition (Civil) No. 853 Of 2021, Writ Petition (Civil) No. 851 Of 2021, Writ Petition (Civil) No. 890 Of 2021 (October 27, 2021).

[76] U.S. Department of Commerce, *Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities* (3 November 2021) https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list

[77] The European Union has also adopted new export controls rules on surveillance technologies. Human Rights Watch, *EU: Robustly Carry Out New Surveillance Tech Rules: Updated Regulations Aim to Restrict Sales to Abusive Governments* (25 March 2021) https://www.hrw.org/news/2021/03/25/eu-robustly-carry-out-new-surveillance-tech-rules#

with an individual's digital data, including the data and contacts of others. At a minimum, the existence and use of Pegasus software likely is unable to come into compliance with international law without sufficient disclosure of its purchase, how it will be deployed, and the extent of data that will be retrieved using the spyware.

41. I conclude by urging the Court to restrain the Government's use of spyware such as but not only Pegasus. It should be encouraged, at a minimum, to impose a moratorium on spyware like Pegasus until global regulation ensures spyware technologies can adhere to human rights obligations; require the Government to disclose the purchase and use of spyware; make the use of spyware subject to independent judicial controls in accordance with clear, human rights compliant law; and remove barriers to trans-national litigation to ensure effective remedies for targeted surveillance.

DEPONENT

VERIFICATION:

I, the deponent do hereby verify that the contents of this affidavit are true and correct to the best of my knowledge and belief. It conceals nothing and no part thereof is false.

Verified at _____on this the _____day of December, 2021.

DEPONENT