ROBERT F. KENNEDY HUMAN RIGHTS

Targeted Surveillance: How NSO Group's Pegasus Spyware Threatens Human Rights

Briefing Paper - August 2021

In light of the Pegasus Project's recent revelations, RFK Human Rights offers a brief analysis of the ways in which the use of spyware by governments to target human rights defenders, activists, and journalists may violate State obligations under existing international human rights legal standards.

Introduction

Pegasus, a spyware developed and sold by Israeli company NSO Group, has been used to surveil human rights defenders, journalists, and dissidents around the globe and has been used as a tool to facilitate human rights abuses. The spyware is secretly installed on victims phones and provides the attacker full access to messages, emails, camera, microphone, and contacts on the phone. This spyware is not new - in fact, investigations led by Citizenlab and the University of Toronto in 2017 documented its use in Mexico against several journalists and activists, which allegedly led the Justice Ministry of Mexico to end its use of the spyware.[1] However, the recent investigation by Amnesty International and Forbidden Stories into the leak of 50,000 phone numbers of potential surveillance targets revealed just how widespread and pervasive the abuse of surveillance technology is today.[2] The Pegasus Project, a collaboration between journalists and media organizations from around the world, revealed that there are suspected clients of NSO in 11 countries including Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, Togo, and the United Arab Emirates (UAE).[3] Users of the Pegasus spyware have utilized it to surveil journalists and activists, with the ultimate goal of silencing them and quashing dissent.[4] So far, the investigation has identified 180 journalists[5] and numerous other human rights defenders who were selected for possible targeting with NSO spyware. These include evidence that family members of Saudi journalist Jamal Khashoggi were targeted with Pegasus software before and after his murder,[6] and that the daughter of political activist Paul Rusesabagina was targeted with Pegasus software after the Rwandan government kidnapped and arbitrarily detained him.[7]

These recent findings have exposed the breadth of abuses throughout the private surveillance industry, including other spyware beyond Pegasus such as Candiru, as well as the failure of States to protect people from this invasive technology.[8] Such violations of the right to privacy inherently implicate other human rights and civic space concerns, making the impact of such abuses particularly egregious and widespread.

---

[1] *How Mexico's traditional political espionage went high-tech,* The Washington Post (July 21, 2021), https://www.washingtonpost.com/world/2021/07/21/mexico-nso-pegasus/.
[2] *Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally,* Amnesty International (July 18, 2021), https://www.amnesty.org/en/latest/news/2021/07/the-pegasus-project/.
[3] *Id.*
[4] *The Pegasus Project*, Forbidden Stories, https://forbiddenstories.org/case/the-pegasus-project/.
[5] *The Pegasus Project*, Forbidden Stories ,https://forbiddenstories.org/case/the-pegasus-project/.
[6] *Jamal Khashoggi's wife targeted with spyware before his death*, The Washington Post (July 18, 2021), https://www.washingtonpost.com/investigations/interactive/2021/jamal-khashoggi-wife-fiancee-cellphone-hack/.
[7] *Hotel Rwanda activist's daughter placed under Pegasus surveillance*, The Guardian (July 19, 2021), https://www.theguardian.com/news/2021/jul/19/hotel-rwanda-activist-daughter-pegasus-surveillance.
[8] *Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus*, The Citizen Lab (July 15, 2021), https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/.

ROBERT F. KENNEDY HUMAN RIGHTS

The UN High Commissioner for Human Rights said that, "technology-enabled surveillance poses significant risks to the enjoyment of human rights in peaceful assemblies and is an important contributor to the shrinking of civic space in many countries."[9]

The Fundamental Right to Privacy

The use of spyware most prominently implicates the human right to privacy, enshrined in the Universal Declaration of Human Rights (UDHR) under article 12 and the International Covenant on Civil and Political Rights (ICCPR) under article 17.[10]

Article 12 of the UDHR states that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to protection of the law against such interference or attacks."[11] Similarly, Article 17 of the ICCPR, which is binding on States, provides that "no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour or reputation" and that "everyone has the right to the protection of the law against such interference or attacks."[12] Article 17 of the ICCPR permits interference with the right to privacy only where it is "authorized by domestic law that is accessible and precise and that conforms to the requirements of the Covenant," has a "legitimate aim," and "meets the tests of necessity and proportionality."[13]

The Right to Privacy and its Implications for the Right to Freedom of Expression

The violation of the right to privacy through targeted surveillance is deeply intertwined with the repression of the rights to freedom of expressions and association, and the importance of the right to privacy is further heightened when freedom of expression is also threatened. Article 19 of both the UDHR and ICCPR protect the right to hold opinions without interference and to seek, receive, and impart information through any media. Article 19(3) establishes a three-part test that requires restrictions on this right to be provided by law and be necessary to protect the rights or reputation of others, national security or public order, or public health or morals.[14]

---

[9] U.N. High Commissioner for Human Rights, Report: Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests, ¶ 24, U.N. Doc. A/HRC/44/24 (June 24, 2020), *available at* https://undocs.org/A/HRC/44/24.

[10] Universal Declaration of Human Rights, Article 12, *available at* https://www.un.org/en/about-us/universal-declaration-of-human-rights; International Covenant on Civil and Political Rights, Article 17, *available at* https://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx.

[11] Universal Declaration of Human Rights, Article 12, *available at* https://www.un.org/en/about-us/universal-declaration-of-human-rights.

[12] International Covenant on Civil and Political Rights, Article 17, *available at* https://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx; Treaties, such as the ICCPR, are legally binding upon States, while other instruments such as the UDHR, although not initially binding, have become incorporated into customary international law, which all States are obliged to follow. For further information on different types of international law and their obligations, please see: https://www.law.georgetown.edu/wp-content/uploads/2019/08/A-Guide-to-the-Basics-of-Intl-Law.pdf.

[13] U.N. Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, ¶ 30, U.N. Doc. A/HRC/69/397 (Sept. 23, 2014), *available at* https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf?OpenElement.

[14] Human Rights Committee, CCPR General Comment No. 34: Article 19: Freedoms of opinion and expression, ¶ 5-9 and 22-36, U.N. Doc. CCPR/C/GC/34 (Sept. 12, 2011), *available at* https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.

ROBERT F. KENNEDY HUMAN RIGHTS

Article 19(3) obligations are triggered even when there is merely a possibility of an interference with communications data.[15] According to General Comment No. 16, a document which interprets and clarifies various provisions of the ICCPR produced by the Human Rights Committee, compliance with Article 17 requires that the confidentiality of correspondence, whether electronic or otherwise, should be guaranteed de jure and de facto.[16] Further, a report from the United Nations High Commissioner for Human Rights states that, "...the collection and retention of communications data amounts to an interference with privacy whether or not those data are subsequently consulted or used. Even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights…"[17]

Violations of the Right to Privacy and Implications on the Right to Freedom of Expression

The former United Nations Special Rapporteur on the promotion and protection of the right to freedom of expression and opinion, David Kaye, noted, "While these principles apply in all cases of targeted surveillance, they have a particular force when expression in the public interest is implicated. Targeted surveillance creates incentives for self-censorship and directly undermines the ability of journalists and human rights defenders to conduct investigations…".[18] General Comment No. 34, interpreting ICCPR Article 19 freedoms of opinion and expression, further holds that under no circumstances can the restrictions to the right under Article 19(3) be used to justify "the muzzling of any advocacy of multi-party democracy, democratic tenets and human rights.".[19] The Human Rights Committee emphasizes the specific importance of protecting journalists and human rights defenders in the face of surveillance.[20] In a recent statement regarding the Pegasus Project revelations, the UN High Commissioner for Human Rights emphasized that, "surveillance measures can only be justified in narrowly defined circumstances, with a legitimate goal and they must be both necessary and proportionate to that goal."[21]

Regional instruments further oblige States to protect individuals and human rights defenders from targeted surveillance. The African Commission on Human and Peoples' Rights requires that States prevent unlawful surveillance undertaken by both State and non-State actors and that any targeted

[15] U.N. High Commissioner for Human Rights, The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights, ¶ 20, U.N. Doc. A/HRC/27/37 (June 30, 2014), *available at* https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf; See also Global Justice Clinic NYU School of Law, Attempted Digital Surveillance as a Completed Human Rights Violation: Why Targeting Human Rights Defenders Infringes on Rights (March 1, 2019) available at, https://chrgj.org/wp-content/uploads/2019/05/190301-GJC-Submission-on-Surveillance-Software.pdf.

[16] Human Rights Committee, CCPR 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, U.N. Doc. HRI/GEN/1/Rev.9 (Vol. I) (April 8, 1988), *available at* https://www.refworld.org/docid/453883f922.html.

[17] U.N. High Commissioner for Human Rights, The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights, ¶ 20, U.N. Doc. A/HRC/27/37 (June 30, 2014), *available at* https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf.

[18] U.N. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Surveillance and human rights: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, ¶ 26, U.N. Doc. A/HRC/41/35 (May 28, 2019), *available at* https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F41%2F35&Language=E&DeviceType=Desktop.

[19] Human Rights Committee, CCPR General Comment No. 34: Article 19: Freedoms of opinion and expression, ¶ 23, U.N. Doc. CCPR/C/GC/34 (Sept. 12, 2011), *available at* https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.

[20] *Id.*

[21] *Use of spyware to surveil journalists and human rights defenders Statement by UN High Commissioner for Human Rights Michelle Bachelet*, U.N. Office of the High Commissioner for Human Rights (July 19, 2021), *available at* https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27326&LangID=E.

surveillance complies with international human rights standards and provides adequate safeguards for the right to privacy.[22] In the Americas, the Office of the Special Rapporteur for Freedom of Expression for the Inter-American Commission on Human Rights has also recognized that unlawful surveillance activity can both directly and indirectly restrict freedom of expression.[23] The Inter-American human rights system urges States to implement laws that limit their own power to surveil private communications.[24] In a joint declaration from the U.N. Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, they declare, "Any surveillance of communications and interference with privacy that exceeds what is stipulated by law, has ends that differ from those which the law permits, or is carried out clandestinely must be harshly punished. Such illegitimate interference includes actions taken for political reasons against journalists and independent media."[25]

NSO Group's Pegasus spyware is secretly installed on victims phones and provides the attacker full access to messages, emails, camera, microphone, and contacts on the phone. Many of those targeted by this surveillance are journalists, human rights defenders, activists, and politicians. Such targeted surveillance is in violation of the ICCPR's article 17 right to privacy because the spyware is being used to interfere with privacy, family, home, and correspondence. The application of the Pegasus spyware would likely not constitute an article 19(3) permissible interference with the right to privacy because it is not authorized by domestic law, is not in conformity with the Covenant, does not have a legitimate aim, and does not meet the necessity and proportionality tests.[26] Further, in light of the damaging effects the unlawful targeted surveillance has had on freedom of expression, including its involvement in the killings and arrests of journalists,[27] Article 17 of the ICCPR has "a particular force" and Article 19(3) cannot be used as a justification.[28]

State Obligations

Duty to Protect Individuals From Surveillance

Despite some uncertainty over the extent of State obligations to protect individuals from targeted surveillance, a legal framework does exist that can serve as a foundation to hold States accountable, both for targeted surveillance conducted by States themselves, as well as for protecting individuals from third-party surveillance and private surveillance companies. Under Article 2 of the ICCPR, States have a

---

[22] The African Commission on Human and Peoples' Rights, Declaration of Principles on Freedom of Expression and Access to Information in Africa, Principles 20, 41 (Nov. 2019), available at https://www.achpr.org/public/Document/file/English/Declaration%20of%20Principles%20on%20Freedom%20of%20Expression_ENG_2019.pdf.

[23] United Nations Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression, Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Joint Declaration on Surveillance Programs and their Impact on Freedom of Expression, ¶ 150 (June 21, 2013), available at, http://www.oas.org/en/iachr/expression/docs/reports/2014_04_08_Internet_ENG%20_WEB.pdf.

[24] *Id* at ¶ 6.

[25] *Id* at ¶ 10.

[26] *Uncovering the Iceberg: The Digital Surveillance Crisis Wrought by States and the Private Sector*, Amnesty International (July 2021), *available at*, https://www.amnesty.org/download/Documents/DOC10449120 21ENGLISH.PDF.

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

[28] U.N. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Surveillance and human rights: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, ¶ 26, U.N. Doc. A/HRC/41/35 (May 28, 2019), *available at* https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F41%2F35&Language=E&DeviceType=Desktop.

duty to protect individuals from third-party interference and to ensure that all rights in the Covenant are recognized and protected.[29] The UN Committee on Economic, Social and Cultural Rights (CESCR) also held that States have the obligation to prevent companies domiciled there from causing or contributing to human rights abuses, even if they occur in other countries.[30] While former U.N. Special Rapporteur David Kaye said that it is unclear whether States have an affirmative obligation to provide legal protection against targeted surveillance,[31] the U.N. General Assembly has specifically declared that the "surveillance of digital communications must be consistent with international human rights obligations and must be conducted on the basis of a legal framework, which must be publicly accessible, clear, precise, comprehensive and non-discriminatory."[32] Further, the Human Rights Committee has held that the right to privacy requires independent oversight on the part of the State, especially in regards to surveillance.[33] The Committee states that such independent oversight includes mechanisms that oversee the export of surveillance products and equipment, ensuring that the judiciary is involved with the authorization of measures and regulations regarding surveillance, affording remedies to individuals attacked by targeted surveillance, and ensuring that all corporations under its jurisdiction comply with domestic and international human rights laws.[34]

U.N. Guiding Principles on Business and Human Rights (UNGPs)

The U.N. Guiding Principles on Business and Human Rights (UNGPs), a set of guidelines for States and businesses to prevent and address human rights abuses, further declares that a State has a duty to protect individuals, which includes the duty to "take appropriate steps to prevent, investigate, punish and redress human rights abuses by third parties."[35] In particular, the Guiding Principles urge States to "exercise adequate oversight to meet their international human rights obligations" especially when they are contracting with businesses whose work may impact human rights.[36]

Alleged Violations by States Implicated in Pegasus Spyware Revelations

So far, the Pegasus Project has identified suspected NSO clients in 11 countries. The large-scale targeting of family, friends, and colleagues of journalists and human rights defenders in those countries has shown such States blatant disregard for human rights and the impunity with which they have been able to use and abuse such spyware. These States have likely violated article 2 of the ICCPR and flouted the principles

---

[29] International Covenant on Civil and Political Rights, Article 2, *available at* https://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx

[30] U.N. Committee on Economic, Social, and Cultural Rights, CESCR General Comment 14: State obligations under the International Covenant on Economic, Social and Cultural Rights in the context of business activities, ¶ 63, UN Doc. E/C.12/GC/24, § III.C.2 (August 10, 2017), *available at* https://www.refworld.org/docid/5beaecba4.html.

[31] U.N. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Surveillance and human rights: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, ¶ 27, U.N. Doc. A/HRC/41/35 (May 28, 2019), *available at* https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F41%2F35&Language=E&DeviceType=Desktop.

[32] U.N. General Assembly, The right to privacy in the digital age, U.N. Doc. A/RES/73/179 (January 19, 2021) *available at* https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/449/97/PDF/N1844997.pdf?OpenElement.

[33] Human Rights Committee, Concluding observations on the sixth periodic report of Italy, ¶ 36, U.N. Doc. CCPR/C/ITA/CO/6 (May 1, 2017) *available at*, https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR/C/ITA/CO/6&Lang=En.

[34] *Id* at ¶ 37.

[35] Human Rights Council, Report of the Special Representative of the Secretary- General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie: Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, U.N. Doc. A/HRC/17/31 *available at*, https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F17%2F31&Language=E&DeviceType=Desktop.

[36] *Id.*

ROBERT F. KENNEDY HUMAN RIGHTS

laid out in the UNGPs by not only failing to protect the victims of this unlawful targeted surveillance, but by actively attacking these victims and stifling civic space. Following the Pegasus Project findings, numerous human rights organizations[37], including RFK Human Rights, have called for a moratorium on the sale and use of surveillance technology.[38]

Responsibilities of Corporations

A culture of widespread secrecy prevails throughout the private surveillance industry along with a lack of accountability, frequently resulting in rampant abuse and human rights violations. The UNGPs provide a framework for businesses to assess whether they are in compliance with international human rights standards. The framework emphasizes establishing policy commitments to respect human rights, due diligence processes to identify, prevent, mitigate and account for human rights impacts, consultation with affected groups, evaluation of human rights policies, and effective grievance mechanisms.[39] The UN High Commissioner for Human Rights, has said that, "companies involved in the development and distribution of surveillance technologies are responsible for avoiding harm to human rights."[40]

Despite this, few companies in the surveillance industry abide by the basic tenets of the UNGPs.[41] In particular, the NSO Group claims that they operate with a Business Ethics Committee and on their website they state that they will "investigate any credible allegation of product misuse", but it is unclear whether "misuse" accounts for human rights violations.[42] Agnès Callamard, Secretary General of Amnesty International said that NSO Group claims that they use Pegasus for "legitimate criminal and terror investigations," but the Pegasus Project disclosures, "blow that premise wide open."[43]

Conclusion

The Pegasus Project, beyond revealing the scope and widespread nature of the use of surveillance technology and the resulting human rights violations, has also exposed the gaps in the framework of international human rights laws and standards for States and businesses. States continue to unlawfully surveil victims with impunity. As Amnesty International notes, "Importantly, it must be recognized that **there is no use** of a targeted digital surveillance tool such as Pegasus that does not implicate the

---

[37] *Unchecked Spyware Industry Enables Abuses: Governments Should Halt Trade in Surveillance Technology*, Human Rights Watch (July 30, 2021), *available at*, https://www.hrw.org/news/2021/07/30/unchecked-spyware-industry-enables-abuses.

[38] *Joint open letter by civil society organizations and independent experts calling on states to implement an immediate moratorium on the sale, transfer and use of surveillance technology*, Amnesty International (July 2021), https://www.amnesty.org/download/Documents/DOC1045162021ENGLISH.PDF.

[39] Human Rights Council, Report of the Special Representative of the Secretary- General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie: Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, ¶ 15-25, U.N. Doc. A/HRC/17/31 *available at*, https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F17%2F31&Language=E&DeviceType=Desktop.

[40] *Use of spyware to surveil journalists and human rights defenders Statement by UN High Commissioner for Human Rights Michelle Bachelet*, U.N. Office of the High Commissioner for Human Rights (July 19, 2021), *available at* https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27326&LangID=E.

[41] U.N. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Surveillance and human rights: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, ¶ 31, U.N. Doc. A/HRC/41/35 (May 28, 2019), *available at* https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F41%2F35&Language=E&DeviceType=Desktop.

[42] See NSO statement of 17 September 2018. See www.nsogroup.com/about.

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

internationally recognized right to privacy, and by implication, often many other rights."[44] While a human rights law framework exists, it needs to be strengthened in order to enforce such limitations and regulations of surveillance tools. Many countries use the guise of national security to continue perpetrating such abuses while failing to demonstrate sufficient legality, necessity, proportionality or legitimate aim.[45] In particular, NSO Group, Israel, and other States involved are "prioritizing the restriction before the right in providing and/or operating the targeted digital surveillance tool."[46] With the limitation of the right to privacy effectively negating the right, targeted digital surveillance has become a common practice with no accountability to any existing international or domestic legal regime.[47]

With the recent disclosures and industry-wide impunity, urgent changes are needed to bring an end to the unlawful targeted surveillance including: independent oversight for both state and government surveillance activities, remedies for victims of the unlawful surveillance, and greater transparency in the industry as a whole. For example, following the news of India's use of Pegasus spyware, Access Now calls on India to establish an independent mechanism for oversight, to provide a judicial remedy for victims, and to otherwise ensure that their domestic laws comply with the most recent human rights standards.[48] Similarly, in 2019, Former Special Rapporteur David Kaye recommended implementing and enforcing laws at the domestic level in accordance with international human rights law, as well as providing victims with domestic remedies. He also further recommended establishing a public mechanism to oversee and approve surveillance technologies, and proffered the creation of a new mechanism by the Office of the High Commissioner for Human Rights such as a working group focusing on the issue of targeted unlawful surveillance[49].

As revelations of new human rights abuses associated with Pegasus and other similar spyware such as Candiru continue to come to light and as such spyware continues to be acquired by governments, former Special Rapporteur David Kaye's recommendations become increasingly urgent. Through multiple parallel efforts aimed at States and companies, working at both the international and domestic levels, companies like NSO Group will no longer be able to profit from Governments seeking to stifle criticism and dissent and journalists and human rights defenders can continue to pursue their vital work unfettered. Until such frameworks are in place, RFK Human Rights will continue to join the calls from Amnesty International and dozens of other human rights organizations for an immediate end to the sale and use of surveillance technology and a thorough, independent investigation into cases of targeted surveillance.

---

[44] *Uncovering the Iceberg: The Digital Surveillance Crisis Wrought by States and the Private Sector*, Amnesty International (July 2021), *available at*, https://www.amnesty.org/download/Documents/DOC1044912021ENGLISH.PDF.
[45] *Id* at 12.
[46] *Id* at 12.
[47] *Id* at 13.
[48] *Policy explainer brief: the Pegasus Project revelations in India*, AccessNow, *available at*, https://www.accessnow.org/cms/assets/uploads/2021/07/India_Parliament_Brief_Explainer_Pegasus_Project.pdf.
[49] U.N. Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Surveillance and human rights: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, ¶ 65, U.N. Doc. A/HRC/41/35 (May 28, 2019), *available at* https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F41%2F35&Language=E&DeviceType=Desktop.