Date: 24 January 2022 Index Number: IOR 40/5179/2022

RIGHT TO FREEDOM OF OPINION AND EXPRESSION: THREATS TO MEDIA POSED BY UNLAWFUL TARGETED SURVEILLANCE

SUBMISSION TO THE UN SPECIAL RAPPORTEUR ON THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION FOR A REPORT TO THE 50TH SESSION OF THE HUMAN RIGHTS COUNCIL

Amnesty International submits this document in response to the call for comments[1] issued by the UN Special Rapporteur on the Right to Freedom of Opinion and Expression to inform her report to the 50th session of the Human Rights Council. While there are several challenges and threats to media in the digital age, this submission is specifically focused on the threat that unlawful targeted surveillance poses to journalists. It contains global trends and includes some country examples. The submission should not be seen as an exhaustive account of the organization's research on these matters.

INTRODUCTION

States' unlawful use of targeted surveillance technologies against journalists and other members of civil society has caused a digital surveillance crisis. States use unlawful surveillance alongside a range of other tactics to silence journalists and impose a chilling effect on civil society. This poses a grave threat to the safety and security of journalists around the world. The consequences for media freedoms are dire. States have failed not only in their obligations to protect journalists from these human rights violations, but have themselves failed in their own human rights obligations, clearly letting these invasive weapons loose on people worldwide for no other reason than exercising their human rights and doing work to protect the rights of others.

This global trend of using targeted surveillance technologies like spyware to clamp down on the rights to freedom of opinion and expression is facilitated by the private surveillance industry. As we noted in our previous submission in February 2019 to the former UN Special Rapporteur on the Right to Freedom of Opinion and Expression, the international surveillance industry is unchecked. Existing standards, oversight and control mechanisms at the domestic, regional, and global levels have proved to be inadequate to prevent human rights violations, and ineffective in providing accountability and remedy.[2]

Unlawful targeted surveillance violates the right to privacy and the rights to freedom of expression, opinion, association, and peaceful assembly, which are protected by both the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). The ICCPR upholds the right to hold opinions without interference and guards against arbitrary and unlawful intrusion on privacy.[3]

International law and standards also require that any interference by the state on the right to privacy should be lawful, necessary, proportionate, and legitimate. States' current practice of unchecked deployment of these tools does not meet these tests. Targeting of journalists and human rights defenders with these technologies solely because of their work is unambiguously unlawful under international human rights law.[4]

This submission will go into the details of how unlawful targeted surveillance has been used to against journalists and suggest pathways to end the practice.

---

[1] Call for comments: Opportunities, Challenges, and Threats to Media in the Digital Age, https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Report-Media-Digital-Age.aspx

[2] Amnesty International, The Surveillance Industry and Human Rights: Amnesty International submission to United Nations Special Rapporteur on the Promotion and Protection of The Right to Freedom of Opinion and Expression (22 February 2019, Index: TIGO IOR 40/9868/2019), https://www.ohchr.org/Documents/Issues/Opinion/Surveillance/AMNESTY%20INTERNATIONAL.pdf

[3] Article 17 and 19, ICCPR

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

USE OF UNLAWFUL TARGETED SURVEILLANCE AGAINST JOURNALISTS

In recent years, cases started to emerge about the use of unlawful targeted surveillance against journalists. From the earlier reports of the use of wiretapping, to phishing attempts, to SMS messages containing malicious links, to now more sophisticated targeted attacks like zero-click spyware. As technologies have evolved, so have the tactics of targeted digital repression. Journalists are hence, faced with new threats which are harder to protect against, harder to detect, and harder still to seek accountability for.

Around the world, there are numerous instances of targeted surveillance technologies being used against journalists. In the UK, reports suggest that the police have put journalists under digital surveillance.[5] In Colombia the national police are reported to have subjected radio journalists to digital surveillance.[6] The research organisation Citizen Lab documented digital attacks against journalists by various threat actors in China, Russia, Ethiopia, and Mexico over the years.[7] Amnesty International has also previously documented malware attacks against bloggers from Viet Nam and a journalist from India.[8] In 2020, Citizen Lab further identified that the notorious surveillance vendor NSO Group's Pegasus spyware was to hack into the personal phones of 36 staff at Al Jazeera, one journalist at Al Araby TV and one journalist at the New York Times.[9] Amnesty International's Security Lab identified evidence of the targeting of Maati Monjib, co-founder of the Moroccan Association for Investigative Journalism and of Omar Radi, a now imprisoned prominent activist and journalist from Morocco using NSO Group's tools.[10]

Following from these earlier reports, The Pegasus Project (the Project) went public in July 2021. The scale and breadth of findings in the Project, drove home just how serious a threat unlawful targeted surveillance poses to press freedom. The project was a collaboration by more than 80 journalists from 17 media organizations in 10 countries coordinated by Forbidden Stories, a Paris-based media non-profit, with the technical support of Amnesty International, who conducted forensic tests on mobile phones to identify traces of the spyware. The Project laid bare how just one surveillance vendor, NSO Group's spyware has been used by state clients to facilitate human rights abuse around the world on a massive scale. The project identified potential NSO clients in 11 countries: Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, Togo, and the United Arab Emirates (UAE). The revelations prove wrong any claims by NSO that such attacks are rare or anomalous, or arising from rogue use of their technology. While the company asserts its spyware is only used for legitimate criminal and terror investigations, it has become clear that its technology facilitates systemic abuse, into which the company appears to be complicit.[11]

At the time of publication in July, the media houses identified at least 180 journalists in 20 countries who were selected for potential targeting with NSO spyware between 2016 to June 2021.[12] At least 25 Mexican journalists were selected for potential targeting over a two-year period, including investigative journalist Carmen Aristegui who was targeted.[13] Pegasus has been used in Azerbaijan, a country where only a few independent

[5] Dominic Ponsford, "Surveillance court says Met grabs of Sun reports' call records 'not compatible' with human rights law," 17 December 2015, www.pressgazette.co.uk/surveillance-court-says-met-was-right-grab-sun-journalists-call-records-hunt-plebgate-sources/

[6] Committee for the Protection of Journalists, 'Claims police spied on two journalists revive surveillance fears of Colombia's press', 2016, https://cpj.org/blog/2016/02/claims-police-spied-on-two-journalists-revive-surv.php

[7] See Marczak et.al., The Great iPwn, December 2020, (https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/) and Marczak et.al., Stopping the Press New York Times Journalist Targeted by Saudi-linked Pegasus Spyware Operator, January 2020, (https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/)

[8] See Amnesty International, Click and Bait: Vietnamese Human Rights Defenders Targeted with Spyware Attacks, February 2021 (https://www.amnesty.org/en/latest/research/2021/02/click-and-bait-vietnamese-human-rights-defenders-targeted-with-spyware-attacks/) and Amnesty International, India: Human Rights Defenders Targeted by a Coordinated Spyware Operation, June 2020, (https://www.amnesty.org/en/latest/research/2020/06/india-human-rights-defenders-targeted-by-a-coordinated-spyware-operation/)

[9] Marczak et.al., The Great iPwn, December 2020, https://citizenlab.ca/2020/12/the-great-ipwn-journalists-hacked-with-suspected-nso-group-imessage-zero-click-exploit/

[10] See Amnesty International, Morocco: Human Rights Defenders Targeted with NSO Group's Spyware, October 2019, (https://www.amnesty.org/en/latest/research/2019/10/morocco-human-rights-defenders-targeted-with-nso-groups-spyware/) and Amnesty International, Moroccan Journalist Targeted With Network Injection Attacks Using NSO Group's Tools, June 2020 (https://www.amnesty.org/en/latest/research/2020/06/moroccan-journalist-targeted-with-network-injection-attacks-using-nso-groups-tools/)

[11] Amnesty International, Scale of secretive cyber surveillance 'an international human rights crisis' in which NSO Group is complicit, July 2021 https://www.amnesty.org/en/latest/news/2021/07/pegasus-project-spyware-digital-surveillance-nso/ (Press Release)

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

[13] Phineas Rueckert, Pegasus: The new global weapon for silencing journalists, July 2021, https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/

media outlets remain. More than 40 Azerbaijani journalists were selected as potential targets according to the investigation. In India, at least 40 journalists from nearly every major media outlet in the country were selected as potential targets between 2017-2021.The investigation also identified journalists working for major international media including the Associated Press, CNN, The New York Times and Reuters as potential targets.[14]

Through forensic tests, Amnesty International's Security Lab confirmed the targeting and/or infections of the devices of numerous journalists. In Azerbaijan, the phones of journalists Sevinc Vaqifqizi and Khadija Ismayilova were infected with Pegasus spyware. In India, forensic tests revealed the phones of journalists Siddharth Varadarajan, MK Venu, Paranjoy Guha Thakurta, Sushant Singh, and SNM Abdi to be infected.In Hungary, journalists Szabolcs Panyi, Daniel Nemeth, András Szabó, Brigitta Csikász, and media owner Zoltan Pava's[15] phones were found to be infected.Journalists based In France including Hicham Mansouri, Lénaïg Bredoux and Edwy Plenel. [16]

This makes it clear that NSO Group's Pegasus spyware is a weapon of choice in the hands of governments to silence journalists.[17] The use of spyware imposes a chilling effect and an atmosphere of intense fear on those who speak out. Even where the presence of surveillance cannot be proven, the mere suspicion that it exists causes journalists to self-censor. Surveillance poses enormous risks to physical safety and mental well-being of journalists. It also places their sources, colleagues, friends, and family in harm's way. It can have enormous consequences on the everyday lives of those targeted or infected.

In 2017, Amnesty International documented the unlawful targeted surveillance against Galima Bukharbaeva, a journalist from Uzbekistan through a phishing attack on her e-mail. Shortly after the attack, news stories began to appear on websites widely perceived to be aligned with – if not controlled by – the government of Uzbekistan which included information from Galima's private emails. So, when Gulasal Kamolova and Vasiliy Markov, two Uzbekistani journalists, saw their names begin to appear in these articles, they knew they may be in danger. They felt intense anxiety and fear. Within six months of the attack on Galima's e-mail account, both Vasiliy and Gulasal were forced to permanently flee their homes in Uzbekistan and seek asylum abroad.[18]

Friends and family members of the slain Saudi journalist, Jamal Khashoggi, were also targeted with Pegasus spyware before and after his murder despite the NSO Group's continuous denial of involvement. According to Amnesty International's forensic analysis, the iPhone of Khashoggi's Turkish fiancée, Hatice Cengiz, was targeted and successfully infected four days after Khashoggi's murder, and multiple times in the subsequent days. Forensics checks also confirmed that his wife Hanan Elatr was targeted with the spyware, as was his friend, and former director-general of Al Jazeera, Wadah Khanfar whose phone was hacked.[19]

These cases exemplify how entire networks of people can be put under surveillance and that surveillance can be tied to grave human rights abuse. Indeed, many of the journalists known be targeted and/or infected by Pegasus have faced a history of repression at the hands of governments, including harassment, smear campaigns, and imprisonment. For journalists who are women, the threat of surveillance is graver still. Information obtained through unlawful surveillance can be weaponised against them through smear

[14] Amnesty International, Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally, July 2021, https://www.amnesty.org/en/latest/news/2021/07/the-pegasus-project/ (Press Release)
[15] Omer Benjakob, The NSO File: A Complete (Updating) List of Individuals Targeted With Pegasus Spyware, January 2022, https://www.haaretz.com/israel-news/MAGAZINE-nso-pegasus-spyware-file-complete-list-of-individuals-targeted-1.10549510
[16] Amnesty International, Forensic Methodology Report: Pegasus Forensic Traces per Target, July 2021, https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-appendix-d/
[17] Phineas Rueckert, Pegasus: The new global weapon for silencing journalists, July 2021, https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/
[18] Amnesty International, "We will find you, anywhere": The global shadow of Uzbekistani surveillance, March 2017, (EUR 62/5974/2017), https://www.amnesty.org/en/documents/eur62/5974/2017/en/
[19] Amnesty International, Forensic Methodology Report: Pegasus Forensic Traces per Target, July 2021, https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-appendix-d/

campaigns, doxing, and other digital attacks. Thus, surveillance is a form of violence against women.[20] Additionally, as we have seen in many cases revealed in the Pegasus Project, even when journalists may choose to leave their countries of origin, the surveillance follows. This makes unlawful targeted surveillance a tool for transnational repression, giving rise to the feeling that nowhere is safe.

Disclosures that began with the Pegasus Project snowballed into a year of blowing the lid on the spyware industry, due to the work of civil society researchers and Big Tech companies. Due to new disclosures, the list of potential clients of NSO Group now includes Poland, Thailand, El Salvador, Ghana, and Uganda.[21] As recently as January 2022, Citizen Lab and Access Now conducted a joint investigation into Pegasus hacking in El Salvador in collaboration with Frontline Defenders, SocialTIC, and Fundación Acceso. They confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. Targets included journalists at *El Faro*, *GatoEncerrado*, *La Prensa Gráfica*, *Revista Digital Disruptiva*, *Diario El Mundo*, *El Diario de Hoy*, and two independent journalists.[22]

As cases continue to emerge, it is important to note that NSO Group isn't the only company selling these tools. Citizen Lab revealed that an Egyptian exiled journalist is known to have been targeted with Cytrox's tools.[23] Worryingly, the lack of transparency into an industry that continues to operate from the shadows means that the cases listed in the submission are likely to be only a part of the picture and as such, are not intended to be comprehensive.

WAY FORWARD

As we noted in our 2019 submission to former Special Rapporteur, existing regulatory frameworks and redress mechanisms remain ineffective and inadequate.[24] This continues to remain the case even today. We have previously analyzed how domestic laws governing surveillance in many jurisdictions, domestic and regional export control frameworks, and other mechanisms like the Wassenaar arrangement are not fit for purpose in their current form to combat the threat of unlawful targeted surveillance.[25] Even where there have been updates to regulatory mechanisms, such as in the case of the new EU dual-use rules, they do not go far enough[26] and will be effective only when implemented with robust transparency.[27] Indeed, the former UN Special Rapporteur on Freedom of Opinion and Expression noted in his report, "It is insufficient to say that a comprehensive system for control and use of targeted surveillance technologies is broken. It hardly exists."[28]

Companies operating in this sphere do so with opacity and impunity. Indeed, we have repeatedly noted that NSO Group's claims that it respects human rights are meaningless, and its policies and practices are ineffective. Our long engagement with the company shows that cyber-surveillance vendors cannot be trusted to

[20] Access Now and Frontline Defenders, Unsafe anywhere: women human rights defenders speak out about Pegasus attacks, January 2022 https://www.accessnow.org/women-human-rights-defenders-pegasus-attacks-bahrain-jordan/
[21] See: https://www.amnesty.org/en/latest/news/2022/01/poland-use-of-pegasus-spyware-to-hack-politicians-highlights-threat-to-civil-society/ and, https://techcrunch.com/2021/11/24/apple-nso-hacking-notify/, and https://www.primenewsghana.com/politics/stan-dogbe-alleges-state-sponsored-attack-on-his-phone.html
[22] Railton et. al, Project Torogoz Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware, January 2022, https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/
[23] Marczak, et. al, Pegasus vs. Predator Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware, December 2021, https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/
[24] Amnesty International, *The Surveillance Industry and Human Rights: Amnesty International submission to United Nations Special Rapporteur on the Promotion and Protection of The Right to Freedom of Opinion and Expression* (22 February 2019, Index: TIGO IOR 40/9868/2019) https://www.ohchr.org/Documents/Issues/Opinion/Surveillance/AMNESTY%20INTERNATIONAL.pdf
[25] Amnesty International, Operating from the Shadows: Inside NSO Group's Corporate Structure, May 2021, DOC 10/4182/2021, https://www.amnesty.org/en/documents/doc10/4182/2021/en/
[26] Amnesty International, New EU Dual Use Regulation agreement 'a missed opportunity' to stop exports of surveillance tools to repressive regimes, March 2021, https://www.amnesty.org/en/latest/news/2021/03/new-eu-dual-use-regulation-agreement-a-missed-opportunity-to-stop-exports-of-surveillance-tools-to-repressive-regimes/ (Press Release)
[27] Access Now et.al, Human Rights Organizations Call for Robust Implementation of New EU Export Control Rules and Investigation of EU member states' role in Pegasus affair, September 2021, https://www.accessnow.org/cms/assets/uploads/2021/09/Pegasus_Export_Control_Rules_Statement.pdf
[28] Report of the Special Rapporteur on freedom of opinion and expression, UN Doc. A/HCR/41/35, para. 46, https://undocs.org/A/HRC/41/35

regulate themselves. In addition, investors have a role to play in ensuring that they are not contributing to or are not directly linked to human rights abuse by way of their investments into these companies.[29]

Amnesty International reiterates its demand that states impose an immediate moratorium on the sale, transfer, and use of surveillance technology, until human rights respecting regulatory frameworks are in place. We have also, alongside others, called on the European Union impose targeted sanctions against NSO Group.[30] Combating this crisis require multi-faceted action at various levels. Thus, we recall the recommendations for various actors in our report titled, 'Uncovering the Iceberg: The Digital Surveillance Crisis Wrought by States and the Private Sector'.[31]

A culture of impunity specific to targeted digital surveillance has developed that must be urgently countered. The information presented in this submission show just how states' use of the targeted digital surveillance tools supplied is utterly out of control, destabilizing, and threatening to individuals' human rights, including physical safety. The revelations shine a light on an unaccountable industry, and an unaccountable sphere of state practice, that must not continue to operate in their current forms. The rights of journalists to freely express themselves, conduct their work without fear and in safety, and the security of the digital ecosystem as a whole depend on it.

[29] Amnesty International, Operating in the shadows: Investor risk from the private surveillance industry, October 2021, https://www.amnesty.org/en/documents/doc10/4359/2021/en/ (DOC 10/4359/2021)
[30] See: https://www.hrw.org/news/2021/12/03/joint-letter-urging-eu-targeted-sanctions-against-nso-group
[31] Amnesty International, Uncovering the Iceberg: The Digital Surveillance Crisis Wrought by States and the Private Sector, July 2021, https://www.amnesty.org/en/documents/doc10/4491/2021/en/ (DOC 10/4491/2021)