

Submission in the case against NSO Group

Introduction

1. Media Defence (hereinafter MD) is a non-governmental organisation that provides legal support and helps defend the rights of journalists, bloggers, and independent media across the world. It has extensive experience in defending journalists and independent media against criminal and civil claims. As part of its mandate, the proposed Intervener engages in strategic litigation to protect and promote freedom of expression. It has intervened in many cases before the European Court of Human Rights (ECtHR), Inter-American Court of Human Rights, and other international courts.¹ It also represents claimants at the ECtHR in cases where they allege that their electronic devices have been hacked by state agents using Pegasus Spyware.² To date it has filed over twenty cases at the ECtHR against governments on behalf of journalists and human rights defenders who allege those governments used Pegasus spyware to spy on them.
2. MD is very concerned about the impact the use of Pegasus spyware is having on journalists seeking to investigate corruption and other wrongdoing. In particular, it is concerned about the pervasive impact the spyware has on the fundamental rights of journalists, including the right to privacy. NSO itself admits that its spyware has led to violations of “fundamental human rights”.³ Through these comments, MD will provide an overview of how easy it is for operators - state agents and others – to hack electronic devices using Pegasus spyware, and then examine the impact this hacking has on freedom of expression and press freedom.

How Pegasus spyware works

3. The way in which Pegasus spyware works provides a critical insight into the impact it is having on privacy and freedom of expression. In terms of its capability to hack smartphones and other devices, Pegasus spyware has been described as a ‘game-changer’⁴ and as having ‘changed cyberwarfare’.⁵ It has the capability to covertly turn a mobile device into a full-time surveillance device as it grants complete and unrestricted access to all information on the device once it is infected with the spyware.⁶

¹ For example, before the European Court of Human Rights MD has intervened in a number of seminal freedom of expression cases including *Axel Springer AG v Germany* (No.2) (Application no. 48311/10), *Delfi AS v Estonia* (Application no. 64569/09), *Magyar Helsinki Bizottság v Hungary* (Application no. 18030/11), and *Wieder and another v the United Kingdom* (Application nos. 64371/16 and 64407/16).

² See for example, Media Defence, *Media Defence files four cases at the ECtHR concerning use of Pegasus spyware by the Azerbaijan government*, 3 October 2022, available at:

<https://www.mediadefence.org/news/pegasus-spyware-azerbaijan/>

³ NSO, *NSO Transparency and Responsibility Report 2021*, (30 June 2021), available at <https://tinyurl.com/ffeu8k7e>, p. 18

⁴ European Parliament, *European Parliament’s Policy Department for Citizens’ Rights and Constitutional Affairs for the Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware*, (May 2022), available at [https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA\(2022\)732268_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf).

⁵ New York Times, *The New Spy Wars*, (28 January 2021), available at <https://www.nytimes.com/2022/01/28/briefing/pegasus-spyware-espionage-cyberwarfare.html>;

⁶ See for example, Amnesty International, *Forensic Methodology Report: How to catch NSO Group’s Pegasus*, (18 July 2021), available at <https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/>

4. Pegasus spyware is implanted in a mobile device by various means including by the user of the device clicking on a malicious link, or through a wireless transmitter that is located near the phone. Where a malicious text message is used, it will invariably be formulated to elicit a target's interest. Once implanted and installed on the device, Pegasus spyware works by causing the device to communicate with a 'command and control' server operated by the entity that is using the Pegasus spyware. This communication is usually conducted via intermediate proxy servers so that it is extremely difficult, by examining the spyware code, to identify the internet address associated with the 'command and control' server (and thereby to ascertain the identity or location of that server and the entity exercising control).⁷
5. Because Pegasus spyware allows the controller to obtain so-called root privileges, or administrative privileges, on the device, it provides full access to the mobile device camera and microphone, and to the mobile device's geolocation. The individual using the spyware can read, send or receive messages that should be end-to-end encrypted, download stored photos, gather passwords, hear and record voice or video calls.⁸
6. A recently reported key feature of Pegasus spyware - the ability to infect a device through the so-called "zero-click" method. This means that Pegasus spyware, unlike other spyware, does not need to rely on any act by the user of the device in order to be triggered, or rely on "jailbreaking" into the system by removing a manufacturer's access restrictions. Once the device is infected with Pegasus spyware it is extremely difficult to detect and the actions it carries out, such as extracting data, are extremely difficult to establish.⁹
7. NSO marketed Pegasus spyware by emphasising and extolling these features. In NSO's 'Pegasus – Product Description' document, among the features it focuses on, it emphasises: the extraction and ongoing collection of all data stored on or by an infected device; location tracking of the device; interception and recording of voice calls on the device; real-time interception and recording of sounds in the vicinity of the device (by covert activation of the in-built microphone); and real-time interception and recording of images in the vicinity of the device (by covert activation of the in-built camera).¹⁰

Impact on fundamental rights including privacy and freedom of expression

8. The rights most directly threatened by Pegasus spyware and related surveillance technology are free expression and privacy, which are inextricably bound and which international law recognises as foundational.¹¹ Under Article 17 of the International Covenant on Civil and Political Rights (ICCPR) and Article 12 of the Universal Declaration of Human Rights (UDHR) the "arbitrary or unlawful interference with [] privacy, family, home, or correspondence" is prohibited.¹² Article 19 of the ICCPR

⁷ See Amnesty International, *Amnesty International Among Targets of NSO-powered Campaign*, (1 August 2018), available at <https://www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/>

⁸ See EDPS, *Preliminary Remarks on Modern Spyware*, (15 February 2022), available at <https://edps.europa.eu/system/files/2022-02/22-02>.

⁹ Amnesty International, *Forensic Methodology Report: How to catch NSO Group's Pegasus*, (18 July 2021), available at <https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/>

¹⁰ NSO Group, *Pegasus Product Description*, available at <https://s3.documentcloud.org/documents/4599753/NSO-Pegasus.pdf>

¹¹ International Principles of the Application of Human Rights to Communications Surveillance, Electronic Frontier Foundation (May 2014), <https://www.eff.org/files/necessaryandproportionatefinal.pdf>.

¹² The UN General Assembly adopted the UDHR in 1948 and it is customary international law. Thailand ratified the ICCPR in 1996.

and UDHR guarantees the right to freedom of opinion and expression, providing “freedom to seek, receive and impart information and ideas of all kinds . . . without interference.” According to the UN Human Rights Committee General Comment 34,¹³ restrictions on the rights to both freedom of expression and privacy must meet strict requirements of lawfulness, necessity, and proportionality. Restrictions must be provided for by law, necessary for achieving a legitimate aim, and be in proportion to the aim sought to be achieved. The restrictions “may never be invoked as a justification for the muzzling of any advocacy of multi-party democracy, democratic tenets and human rights.”¹⁴ While states often rely on ‘national security’ to justify restrictions, the UN Special Rapporteur on the right to freedom of opinion and expression has found that such justifications should be limited to situations in which the interest of the whole nation is at stake, rather than the interests of the government.¹⁵

9. The UN Human Rights Committee and the UN General Assembly further clarified the application of these principles, determining that state surveillance requires robust and independent judicial oversight, must be carried out under a legal framework, and must remain consistent with international human rights obligations.¹⁶ The UN Human Rights Committee also emphasised the importance of these principles when surveillance targets civil society by creating “incentives for self-censorship” and undermining “the ability of journalists and human rights defenders to conduct investigations and build and maintain relationships with sources of information.”¹⁷
10. NSO’s government clients violate these international laws when they use Pegasus spyware to target individuals simply for exercising their right to expression. Frequently, the laws purporting to authorise surveillance are vague, grant excessive discretion to the authorities, and lack independent judicial oversight.¹⁸
11. The United Nations Guiding Principles on Business and Human Rights (UNGP)¹⁹ recognises that businesses such as the NSO Group are required to take steps to prevent human rights abuses. Section II of the UNGPs requires all businesses to respect human rights, avoid infringing on those rights, and address adverse impacts that they cause or contribute to, independent of any state’s willingness to fulfill its own obligations.²⁰ The UNGP also requires businesses to prevent or reduce adverse human rights impacts directly linked to their operations.²¹ Applying the UNGP to NSO Groups activities, it is required for example to put in place policies to identify human rights commitments, and engage in human rights compliant due diligence.²² Where a violation of rights does take place, companies must

¹³ UN General Assembly, Human Rights Committee, General Comment No. 34, para 22 (Sept. 12, 2011), <https://undocs.org/CCPR/C/GC/34>; see also, e.g., UN General Assembly, Human Rights Council, *The right to privacy in the digital age*, para 2 (April 7, 2017), <https://undocs.org/A/RES/34/7>

¹⁴ General Comment 34 para 23, supra note 13.

¹⁵ UN General Assembly, Human Rights Council, *The right to privacy in the digital age*, supra footnote 13, para 25.

¹⁶ UN General Assembly, Resolution 73/179, “*The right to privacy in the digital age*” (Jan. 21, 2019), <https://undocs.org/en/A/RES/73/179>.

¹⁷ Ibid.

¹⁸ David Kaye, *UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools*, OHCHR (June 25, 2019), <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736>; E. Tendayi Achiume, *UN expert joins call for immediate moratorium on sale, transfer and use of surveillance tech*, OHCHR (July 15, 2020), <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=26098 &LangID=E>.

¹⁹ Guiding Principles on Business and Human Rights, UN Human Rights OHCHR (2011), https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf

²⁰ Ibid. at II.A.11, 13(a).

²¹ Ibid. 13(b).

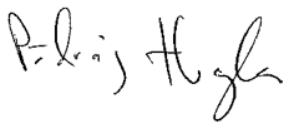
²² Ibid. 15.

act to mitigate the impact of that violations, including by terminating any related business relationship where necessary.²³

12. Despite these requirements, the NSO Group has done nothing to mitigate or prevent the deleterious impact of its spyware, as the UNGP requires it to do.²⁴ The use of Pegasus spyware is, in its very essence, incompatible with freedom of expression, the rule of law, and the principles of democracy.

Conclusion

13. States intent on suppressing freedom of expression, and press freedom in particular, often rely on a campaign of arrest, detention, and prosecution of journalists who have been critical of the government. With Pegasus spyware, surveillance of journalists has become easier. Media Defence is particularly concerned that Pegasus spyware is a different, more insidious, method of surveillance, which effectively grants the controller of the spyware access to almost every facet of the target's life, as well as the lives of family, friends, and, for journalists, sources, contacts, and others who might fear reprisal for their relationship with that journalist.
14. In its effect, it destroys the target's rights to private life and right to free expression. As noted above, once Pegasus spyware is installed remotely on a device, either through fraud or deception, and without its owner's awareness or consent, the controller can then issue commands to the spyware remotely to surveil activities and communications and steal and transmit personal data from the infected device in a variety of ways. Pegasus can record using a device's microphone and camera, track the phone's location data, and collect emails, text messages, browsing history, and a host of other information accessible through the device.
15. It is Media Defence's submission that the use of Pegasus spyware against journalists and human rights defenders as well as others can be considered a wholly excessive restriction on the exercise of fundamental rights.

A handwritten signature in black ink, appearing to read "Pádraig Hughes".

Pádraig Hughes
Legal Director

²³ Ibid. 19.

²⁴ See for example, Al Jazeera, *Israeli firms sold invasive surveillance tech to Indonesia: Report*, 3 May 2024, available at <https://www.aljazeera.com/news/2024/5/3/israeli-firms-sold-invasive-surveillance-tech-to-indonesia-report>