Affidavit

I, the undersigned, Danna Ingleton, I.D. No.____, having been notified that I must tell the truth and nothing but the truth, and that if I do not do so, I will be subject to criminal penalties under the law, hereby declare as follows:

1. I have personal knowledge of the facts set out in this affidavit, except where, as noted, I have relied on the information of others that I believe to be true.
2. My name is Danna Ingleton. I am a lawyer called to the Law Society of Upper Canada, and the Deputy Director of Amnesty Tech, a global program based at the International Secretariat of Amnesty International in London, United Kingdom. Prior to my current position, I worked as a research and policy adviser for Amnesty International on the protection of human rights defenders and civil society. I have worked in the human rights field for over a decade.
3. I submit this affidavit to provide the court with information regarding the misuse of NSO Group's digital surveillance software system against human rights defenders and other members of civil society, including an attempt to infect the mobile device of a staff person at Amnesty International – arguably the world's largest human rights organization – with NSO Group's sophisticated spyware platform, Pegasus. As set forth in this affidavit, the abundance of reports pointing to governments' deployment of the Pegasus spyware platform to surveil human rights defenders, and the absence of evidence that NSO Group has undertaken adequate due diligence and corrective measures or other steps to prevent such foreseeable misuses of its products, demonstrate the basis for Amnesty International's recommendation, with which I agree, that NSO Group's export license must be revoked.

4. In what follows, I first provide a brief overview of the work of Amnesty International pertaining to the digital surveillance industry and protection of human rights defenders. I then discuss the inherent dangerousness of NSO Group's surveillance products and the foreseeability of their misuse when sold to governments that have a history of violating the rights of human rights defenders and that lack adequate legal frameworks for, and institutional oversight of, the deployment of digital surveillance software. Next, I review public reports that multiple dissidents, journalists, human rights defenders including an Amnesty International staff member, and other actors, have been targeted with Pegasus spyware, by governments well known for repressing or failing to protect civil society. I then address NSO Group's apparent failure to take adequate steps to prevent the foreseeable misuse of its products prior to or after their sale, and the Israeli government's apparent failure to adequately prevent such sales – shortcomings that exacerbate the risk of misuse. Finally, I discuss how targeting civil society with surveillance software such as the Pegasus spyware platform infringes on the rights to privacy, freedom of opinion, and freedom of expression, regardless of whether the targeted digital device is ultimately infected.

Amnesty International is a world leader in human rights advocacy and research, including research documenting how misuse of digital surveillance technology violates human rights.

5. Amnesty International is a global organization consisting of over 70 national entities (known as "sections"), the International Secretariat (legally registered in London, U.K.) and over seven million supporters from every part of the world ("Amnesty International"). Founded in 1961, Amnesty International is independent of any government, political ideology, economic interest or religion. Amnesty International

campaigns for the respect, development and progressive realization of international human rights law and international humanitarian law. Its work is predicated on international rules and principles reflected in diverse norms of human rights, including treaties, general principles of international law, and rules of customary international law. Amnesty International also undertakes research, advocacy and litigation highlighting human rights violations, and advancing justice, truth, reparation and guarantees of non-recurrence for victims of human rights violations. In addition to its work on specific cases and patterns of human rights abuses, Amnesty International urges all governments to observe the rule of law and to ratify and implement human rights standards, and encourages all organizations to support and respect human rights.

6. Amnesty Tech is a program of the Amnesty International Secretariat, headquartered in the United Kingdom with globally-distributed staff in Berlin, Beirut, Dakar, Nairobi, New York, Tunis and San Francisco. Amnesty Tech focuses on the intersection of technology and human rights.
7. I have worked with Amnesty International for almost eleven years, supporting the organization's work on the protection of human rights defenders and civil society. I began working as a Deputy Director of Amnesty Tech in 2018. In my capacity as a Deputy Director, I am responsible for Amnesty International's work on surveillance and censorship, and the technological empowerment of civil society and human rights defenders.
8. Through my work to protect human rights defenders, I have observed numerous documented cases of governments' use of digital surveillance to repress human rights defence, free speech and peaceful political dissent. Amnesty International has

documented multiple instances in which state-sponsored digital attacks and surveillance have intimidated and silenced human rights defenders by turning the digital devices that defenders use to protect and promote human rights into tools for tracking their communications, movements, and networks.[1]

9. As part of the organization's ongoing work on the protection of human rights defenders, Amnesty Tech has researched the targeted digital surveillance of human rights defenders and other members of civil society. Through its investigations in 2018, Amnesty International documented the misuse of NSO Group's Pegasus spyware, including against a staff member of Amnesty International.

NSO Group's Pegasus spyware platform threatens individual privacy and security, and its potential misuse in contravention of international human rights law, specifically by governments known to repress human rights defenders, is an entirely foreseeable risk.

10. Because of its covert operation, sophisticated targeting capabilities, and extreme invasiveness, the potential for abuse of the Pegasus spyware platform is foreseeable. Governments that purchase and deploy the Pegasus spyware platform obtain access to targeted individuals' private data, including the ability to secretly control a target's mobile device.[2] Due to the potential security implications of the platform, Pegasus is

[1] See Amnesty International, *Human Rights under Surveillance: Digital Threats Against Human Rights Defenders in Pakistan* (Index: ASA 33/8366/2018), p. 15; Amnesty International, *Meet NSO Group: a go-to company for human rights abusers*, 6 August 2018, www.amnesty.org/en/latest/news/2018/08/is-nso-group-a-goto-company-for-human-rights-abusers/; Amnesty International, *Amnesty International Among Targets of NSO-powered Campaign*, 1 August 2018, www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/

[2] Amnesty International, *Amnesty International Among Targets of NSO-powered Campaign*, 1 August 2018, www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/; Bill Marczak and John Scott-Railton, Citizen Lab, *Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender*, 24 August 2016, section 3, www.citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

regulated by Israel's Defence Export Controls Agency (DECA) under the same type of licensing requirements and export restrictions applicable to military weapons and national security systems.

11. Pegasus reportedly can be installed on a target's mobile device in several ways. Most commonly, it is activated when a target clicks on a specific exploit link, often sent via SMS. Once a target clicks on the link, the system covertly downloads onto the mobile device. **[Exhibit 1a, 1b]** Alternatively, reporting also suggests that NSO Group may have refined techniques to infect a device without any user interaction. According to reporting by Motherboard, NSO Group can allegedly provide full access to the contents of a phone with only the telephone number of a target, without need for a user to click on a malicious link.[3]
12. Once installed, Pegasus allows an operator to access all existing data on the mobile device, including contacts, photos, call history and previous text messages—regardless of encryption or other protections. The spyware platform can actively record or passively gather a variety of different data about and from the device, including communications and location information. Also particularly troubling, Pegasus allows an operator to remotely enable cameras and microphones to record the targets' surroundings and private conversations—essentially converting the device into a sophisticated eavesdropping and tracking tool to be used against them. As Citizen Lab has summarized, "by giving full

[3] Lorenzo Franceschi-Bicchierai and Joseph Cox, Motherboard, *They Got 'Everything': Inside a Demo of NSO Group's Powerful iPhone Malware*, 20 September 2018, motherboard.vice.com/en_us/article/qvakb3/inside-nso-group-spyware-demo/

access to the phone's files, messages, microphone and video camera, the operator is able to turn the device into a silent digital spy in the target's pocket."[4]

13. Despite its potential for abuse, NSO Group has sold its spyware platform to numerous governments known to have repeatedly violated the rights of human rights defenders,[5] as described further below.

The targeting of an Amnesty International staff member for surveillance with the Pegasus spyware platform, on the basis of that individual's human rights work and/or related opinion in violation of human rights law, had a chilling effect on the individual staffer and across Amnesty International's operations.

14. In June 2018, an Amnesty International staff member was the target of an attempted digital attack with surveillance software. As detailed in an online report released by Amnesty International **[Exhibit 1a]** the staff member received a suspicious message over WhatsApp which read: "can you please cover [the protest] for your brothers detained in Saudi Arabia in front of the Saudi Embassy in Washington. My brother was detained in Ramadan and I am on a scholarship here so please do not link me to this. [LINK]." This message was sent to the staff member during a period when Amnesty International was campaigning for the release of six women's rights activists detained in Saudi Arabia.
15. As Deputy Director of Amnesty Tech I work directly with our team of technologists. It is through their work that I learned that the link embedded in the WhatsApp message sent to

[4] Bill Marczak and John Scott-Railton, Citizen Lab, *Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender*, 24 August 2016, section 3.3, www.citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

[5] Bill Marczak et al, Citizen Lab, *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, 18 September 2018, www.citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

my colleague was connected to a domain known to distribute and deploy NSO Group's Pegasus spyware platform. They determined, and I believe to be true, that, had the staff member clicked on the link, the victim would have been taken to what is described as a 'Pegasus Installation Server' which would have attempted the exploitation of the device and the silent installation of the Pegasus spyware on the staff member's smartphone, thus infecting it.[6]

16. Amnesty technologists also determined that the domain that hosted the link in the message was part of a network of digital infrastructure comprising more than 600 suspicious domains[7] used to lure targeted individuals to click on links that trigger infection with Pegasus spyware.[8]

17. The tailored language of the message sent to the Amnesty staff member, which was designed to bait the recipient to open the malicious link, suggests that the staffer was being targeted for surveillance. Although it appears a Pegasus infection of that device was not triggered, the staff member was extremely distressed that they had been targeted on the basis of their human rights work—in clear violation of the right to freedom of opinion, freedom of expression, and the right to privacy, guaranteed under the International Covenant on Civil and Political Rights, as explained below[9]—and that their individual mobile phone had been specifically selected for infection. The "bait message"

[6] Amnesty International, *Amnesty International Among Targets of NSO-powered Campaign*, 1 August 2018, www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/
[7] This list of domains can be found at Github, *Indicators from Amnesty International's investigations*, 1 August 2018, www.github.com/AmnestyTech/investigations/blob/master/2018-08-01_nso/indicators.csv; and RiskIQ PassiveTotal, *Amnesty International: Amnesty among targets of NSO powered campaign*, 1 October 2018, community.riskiq.com/projects/d8ebc1d0-f5a6-d135-3819-45b53a0a2b4b.
[8] Among these we found servers that hosted domain names that Citizen Lab and others have previously identified as connected to NSO Group, namely, banca-movil[.]com, pine-sales[.]com, and ecommerce-ads[.]org. See Bill Marczak et al, Citizen Lab, *NSO Group Infrastructure Linked to Targeting of Amnesty International and Saudi Dissident*, 31 July 2018, www.citizenlab.ca/2018/07/nso-spyware-targeting-amnesty-international/
[9] *See infra*, paras 36-39.

used the staff member's human rights work as a means of deceiving and luring them into the sought action, in an attempt to maliciously infect their device. The staffer's sense of fear following the attempted attack and uncertainty as to whether they were being surveilled not only contributed to the staff member's mental and emotional distress, but also led to insecurity surrounding their human rights work and altered digital behavior. I know well the impact this targeting has had on the staff member, as I have personally held many conversations with them about their experience of the targeting, and about whether or not we can reveal their name in seeking accountability and justice for this targeting. The staff member is not comfortable with their name being released. This chilling effect infringed on the staff member's rights to privacy, as well as freedom of opinion and expression, as I discuss further below.[10]

18. The impacts of the attempted infection extended beyond the individual staff member, imposing costs on the organization as a whole. This incident further highlighted the urgency, within Amnesty International and the human rights sector as a whole, to allocate more resources to mitigate against sophisticated spyware.

The Pegasus spyware platform has been used against civil society actors across the world, including by governments with a history of targeting human rights defenders.

19. The targeting of an Amnesty International staff member's phone in June 2018 was not an isolated incident. The unique identity of the link received by the Amnesty International staffer, and the tailored content of the bait message, fit the pattern observed in other documented digital attacks involving the use of Pegasus. Since August 2016,

[10] *See infra*, paras 36-39.

technologists at both Amnesty International and Citizen Lab have documented repeated abuses of NSO Group's Pegasus spyware platform to target and surveil human rights defenders and other civil society actors.

20. According to research undertaken by Citizen Lab for its report *Hide and Seek* **[Exhibit 15]**, NSO Group's Pegasus spyware platform has been traced to 45 countries where operators of Pegasus may have been functioning between August 2016 and August 2018. Of those 45 countries, Citizen Lab reports that "[a]t least six countries with significant Pegasus operations have previously been linked to abusive use of spyware to target civil society, including Bahrain, Kazakhstan, Mexico, Morocco, Saudi Arabia, and the United Arab Emirates [UAE]." **[Exhibit 15]**

21. For example, Citizen Lab's August 2016 report, *The Million Dollar Dissident* **[Exhibit 16]**, documented attempts to infect the phone of Emirati human rights defender Ahmed Mansoor with the Pegasus spyware platform. Citizen Lab has also uncovered evidence of the targeting of the devices of more than twenty individuals in Mexico – none of whom has been identified or charged as a suspected criminal including by way of alleged involvement in terrorism-related conduct – with Pegasus spyware. *The Million Dollar Dissident* documented the targeting of Mexican journalist Rafael Cabrera **[Exhibit 16]**. *Bitter Sweet*, Citizen Lab's second investigative report published in February 2017 **[Exhibit 17]**, documented the targeting of two Mexican health advocates and a government food scientist pushing for public health measures opposed by soft drink companies. All three victims received malicious SMS links, later confirmed to be overlapping with NSO Group's Pegasus infrastructure. **[Exhibit 17]**. In May 2017, Citizen Lab's *Reckless VI* **[Exhibit 18]** reported the Mexican government's targeting of

two more members of Mexican civil society, both journalists, with infrastructure linked to the Pegasus spyware platform.

22. According to another Citizen Lab report, *The Kingdom Came to Canada* **[Exhibit 19]**, Omar Abdulaziz, a Saudi activist currently residing in Canada who is known to be an outspoken critic of the Saudi government, was targeted and his device infected with NSO Group's Pegasus spyware platform **[Exhibits 20, 6, 21, 5]**. Abdulaziz has publicly stated that he was a friend of murdered journalist Jamal Khashoggi, who was extrajudicially executed inside the Saudi Arabian consulate in Turkey **[Exhibits 6, 20].** Abdulaziz has initiated a lawsuit against NSO Group, asserting that Pegasus was used with the intent to track and collect his extensive communications with Khashoggi **[Exhibits 7, 22, 23]**. The complaint alleges that Pegasus allowed Saudi officials access to the details of collaborations between Khashoggi and Abdulaziz and contributed to Khashoggi's murder **[Exhibit 22]**.

23. These incidents indicate that the Pegasus spyware platform is being used against human rights defenders by governments with long and well-documented histories of repression and abuse, and which lack legal frameworks or oversight mechanisms to authorize and regulate surveillance technology. For example, the Saudi government has a well-documented history of severely restricting the rights to freedom of expression, opinion, association and peaceful assembly, and has long invested in surveillance systems.[11] Surveillance is rampant and authorities monitor political, social and religious activists under the pretext of protecting national security.[12] Many human rights defenders and

[11] Amnesty International, *Human Rights in the Middle East and North Africa: Review of 2018: Saudia Arabia* (Index: MDE 23/9902/2019)
[12] Freedom House, *Freedom on the Net 2018 - Saudi Arabia*, 1 November 2018, www.refworld.org/docid/5be16afc13.html

government critics have been arbitrarily detained for their work and authorities repress dissent both online and offline.[13] The UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism expressed concerns about Saudi Arabia's use of its counter-terrorism law against individuals exercising their rights.[14]

24. In the UAE, the country's most well-known human rights activists are behind bars under the pretext of national security, and fear dissuades many victims of human rights violations and dissidents from speaking freely against government abuse.[15] Media reports indicate that Emirati authorities have previously engaged in widespread digital surveillance of human rights activists critical of the monarchy through programs like 'Project Raven', a secret state hacking operation that reportedly targeted hundreds of activists.[16] Further, there are little to no privacy protections or opportunities for anonymous communication in the UAE.[17]

25. The grave risks facing human rights defenders and journalists in Mexico are likewise well documented. The incidence of attacks on activists, dissidents and journalists, including killings, intimidation, harassment, violence, and disappearance,[18] remains alarmingly high despite reported efforts by the federal government to implement

[13] Amnesty International, *Human Rights in the Middle East and North Africa: Review of 2018: Saudia Arabia* (Index: MDE 23/9902/2019)
[14] Report to the Human Rights Council, Visit to Saudi Arabia, Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN Doc. A/HRC/40/52/Add.2 (2018), www.undocs.org/A/HRC/40/52/Add.2
[15] Report to the Human Rights Council, Compilation on the United Arab Emirates, Office of the UN High Commissioner for Human Rights, UN Doc. A/HRC/WG.6/29/ARE/2 (2017), www.undocs.org/A/HRC/WG.6/29/ARE/2
[16] Christopher Bing and Joel Schectman, Reuters, *Project Raven: Inside the UAE's Secret Hacking Team of American Mercenaries*, 30 January 2019, www.reuters.com/investigates/special-report/usa-spying-raven/
[17] Freedom House, *Freedom on the Net 2018 - United Arab Emirates*, 1 November 2018, www.refworld.org/docid/5be16af0a.html
[18] Amnesty International, *Urgent Action: Indigenous Human Rights Defenders at Risk* (Index: AMR 41/9879/2019)

protections.[19] Moreover, as noted by UN Special Rapporteur on Freedom of Expression, David Kaye, and Special Rapporteur for Freedom of Expression of Inter-American Commission on Human Rights, Edison Lanza, government entities within Mexico have engaged in digital surveillance of journalists, human rights defenders, and others.

26. Given the extensive public documentation of repression of human rights defenders by the governments listed above, NSO Group at least had constructive notice of the foreseeable risk that those governments would misuse its spyware to surveil human rights defenders. When Citizen Lab and other public sources detailed specific instances involving the use of Pegasus technology for unlawful surveillance purposes—particularly where the government repeatedly used Pegasus against human rights defenders, as in the case of Mexico—the company also had actual notice of such misuse.

NSO Group has failed to refute mounting evidence that its technology is being used to target human rights defenders or to undertake adequate due diligence and corrective measures to prevent such abuses.

27. Despite notice of the foreseeable risk that the above-mentioned governments would misuse its spyware to unlawfully surveil human rights defenders, there is no evidence that NSO Group refused to sell its products to those governments, ascertained that those governments had proper legal frameworks and oversight mechanisms for the use of spyware in place prior to any sale, or revoked access to its products after evidence emerged of their misuse. NSO Group has not refuted the accounts that its Pegasus

[19] Organization of American States, *Special Report on the Situation of Freedom of Expression in Mexico*, Joint Report of the Special Rapporteur for Freedom of Expression of IACHR, Edison Lanza, and the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, on their mission to Mexico, June 2018, www.oas.org/en/iachr/expression/docs/2018_06_18_CIDH-UN_FINAL_MX_report_ENG.pdf

spyware platform has been misused to target human rights defenders. Nor has it accepted responsibility and provided remedies for the multiple reported instances of misuse of its surveillance technologies. NSO Group continues to defend itself by stating that its software is intended only for prevention of crime including terrorism-related conduct, despite the evidence that its software is abused. Following reports by the Citizen Lab, Amnesty International, the *New York Times* and other media outlets on the targeting of civil society actors with Pegasus spyware, NSO Group released several public responses **[Exhibits 2, 4, 5, 6, 7, 8]** which have been insufficient to demonstrate the adequacy of the company's preventive or corrective steps.

28. Despite claiming that it conducts investigations of abuse of its software, NSO Group has failed to disclose details regarding the substantive findings of any such investigations conducted in response to reports of misuse or the parameters of its due diligence process. NSO Group has repeatedly stated that its Business Ethics Committee "reviews and approves each transaction" **[Exhibit 2]** and to ensure proper compliance with its policies, but none of NSO Group's public statements has explained the components of its Business Ethics Committee's "rigorous internal compliance process." **[Exhibit 6]** It remains unclear what factors are taken into consideration before the company sells an intrusive and inherently dangerous product, like the Pegasus spyware platform, to an interested government.
29. NSO Group has likewise failed to demonstrate that it has detected any risks, taken any subsequent measure to prevent or minimize these risks, or cancelled or blocked sales due to the foreseeable risk of its products being used against civil society, or upon evidence of such abuses. Although NSO Group has stated that it "is authorized to reject agreements

or cancel agreements where there is a case of improper use" **[Exhibit 2, 3]**, there is no evidence that NSO Group has taken such action following credible reports that its spyware platform has been used against civil society. NSO Group asserts that its Business Ethics Committee has blocked deals in the past three years, but it has not articulated the grounds for doing so or explained what factors the Business Ethics Committee considers prior to taking these decisions **[Exhibit 6,10]**.

30. At a minimum, in order to meet its responsibilities under the *UN Guiding Principles on Business and Human Rights* and address the recommendations of civil society, prior to selling its products, NSO Group should review public information regarding a prospective client government's human rights record with regard to the treatment of civil society, and determine whether the government has an adequate legal framework in place authorizing and regulating the use of digital surveillance technology, which is subject to independent institutional oversight.

31. In addition to such pre-sale due diligence, NSO Group has the capacity and responsibility to monitor the use of its products post-sale, to prevent, mitigate, or take action to discontinue abusive use. News reports and admissions by NSO Group itself contradict the company's claims that it is not involved with the deployment of Pegasus post-sale **[Exhibit 13]**. For example, in June 2017, NSO Group reportedly sold the Pegasus spyware platform to government actors in Saudi Arabia **[Exhibit 9].** Following Saudi Arabia's purchase of the Pegasus spyware platform, Q Cyber Technologies, a holding company of NSO Group, reportedly continued to assist Saudi officials with the implementation and operation of the software, and was directly involved in helping to solve Pegasus-related problems **[Exhibits 7, 5]**. This involvement suggests not only that

NSO Group could do more to prevent the unlawful use of its software against civil society, but also that it has knowledge of how the tool is being used.

32. Moreover, statements from one of NSO Group's CEOs, Shalev Hulio, indicate that NSO Group has knowledge of active Pegasus targets. In an interview with Yedioth Ahronoth, Hulio stated that there were "no more than 150 active targets" of Pegasus. He asserted that it was impossible to deploy Pegasus against a target without NSO Group being able to "check" the deployment **[Exhibit 14]**. These statements suggest that NSO Group has the capacity to identify instances of misuse of the Pegasus spyware platform and take remedial action.

33. Recent investigative reports by Haaretz detailing NSO Group's sale of Pegasus to the Saudi government suggest the company lacks adequate procedures and safeguards regarding the risks its products pose to human rights **[Exhibit 7]**. Despite widespread accounts of the Saudi government's systematic repression of civil society and the lack of a domestic legal framework for, or independent oversight of, the deployment of the spyware system, NSO Group reportedly courted a deal with Saudi officials. A November 2018 Haaretz article **[Exhibit 9]** details the attempts of Saudi officials to buy the Pegasus system, just months before the Saudi Crown Prince's widely reported purge of regime opponents. According to Haaretz, during several overseas meetings between NSO Group and Saudi officials, NSO Group officials touted the capabilities of Pegasus, and "promised" the Saudi officials that Pegasus would be able to access targets in multiple Middle Eastern countries. During an earlier June 2017 meeting, Haaretz reports, NSO Group promoted the sophistication of Pegasus by demonstrating its ability to infect a

phone with nothing more than a phone number; the target was not required to click on a link for the device to become infected **[Exhibit 9]**.

34. Additionally, in a March 2019 televised interview for the investigative program *60 Minutes*, Shalev Hulio did not deny that NSO Group's spyware had been sold to Saudi Arabia when he was questioned specifically on that point **[Exhibit 24]**.

35. That such sales occur raises serious questions not only about NSO Group's internal procedures, but also about whether the oversight exercised by the Israeli Ministry of Defence addresses human rights risks. Because DECA does not publicly disclose the export licenses granted to specific companies, or even comment on whether a valid license exists **[Exhibits 7, 9]**, it is difficult to assess the adequacy of DECA's own procedures to ensure effective protection of human rights in the context of its export licensing processes. In particular, it is difficult to assess whether any human rights screening or risk assessment was performed ahead of granting NSO Group the license that has allowed it to sell its surveillance technology to foreign governments.

Allowing NSO Group to continue selling the Pegasus spyware platform threatens the rights to privacy and to freedom of opinion and expression, in breach of Israel's obligations under international human rights law.

36. The targeting of civil society actors with the Pegasus spyware platform violates the rights to privacy, freedom of opinion and freedom of expression under the International Covenant on Civil and Political Rights (ICCPR), by arbitrarily or otherwise unlawfully invading individuals' privacy on the basis of their opinion or activities protected under

international human rights law,[20] which in turn chills their expressive communications.[21] It further puts in jeopardy the confidentiality and safety of their sources, including victims of human rights violations often putting their life at risk to expose the abuses they have been facing.

37. Under ICCPR Article 19(1), freedom of opinion may never be infringed on, while the rights to privacy and freedom of expression, guaranteed under Articles 17 and 19(2)-(3), respectively, may only be restricted subject to lawful domestic authorization. To prevent abuse of these rights, governments must, at a minimum, implement a domestic legal framework governing the deployment of digital surveillance technology, subject to independent institutional oversight, including the judiciary. Authorization must rest on a clear, publicly accessible law and *each* restriction must be authorized by an independent judiciary. Furthermore, restrictions must be both necessary and proportionate to a legitimate government aim.

38. Regardless of state justifications, human rights defenders, dissidents, and journalists may never be subject to surveillance on the basis of their opinion and/or public interest work. Any effort to coerce an individual to hold or not hold any opinion is prohibited,[22] making the targeting of a human rights defender on the basis of their opinion a violation of their freedom of opinion. As detailed above, numerous reports demonstrate that human rights defenders, including an Amnesty International staffer, have been specifically targeted

[20] Articles 17 and 19 of the International Covenant on Civil and Political Rights (1966); *see also* Human Rights Committee, General Comment 34, Article 19: Freedoms of opinion and expression, UN Doc. CCPR/C/GC/34 (2011), para. 10, www.undocs.org/CCPR/C/GC/34

[21] See Amnesty International, *Human Rights under Surveillance: Digital Threats Against Human Rights Defenders in Pakistan* (Index: ASA 33/8366/2018), p. 15

[22] Human Rights Committee, General Comment 34, Article 19: Freedoms of opinion and expression, UN Doc. CCPR/C/GC/34 (2011), para. 10, www.undocs.org/CCPR/C/GC/34

with the Pegasus spyware platform on the basis of their human rights work and/or related opinion.

39. Attempted digital surveillance of a human rights defender—whether or not successful—is evidence of the unlawful targeting of that individual on the basis of their human rights work and/or related opinion.[23] A digital attack that contains malicious links connected to the distribution and deployment of spyware, regardless of whether infection happens, is therefore a completed act of intimidation in itself. Moreover, given reports that Pegasus can allegedly infect a device through a "zero-click" method and is not detectable once installed, an attempted Pegasus attack gives the targeted individual a reasonable basis to fear that they are subject to surveillance. The targeting of a human rights defender on the basis of their human rights work and/or related opinion also demonstrates that existing due diligence frameworks, export control regimes, and other regulatory measures have failed to protect against human rights violations.

40. Under international standards set out in the *UN Guiding Principles on Business and Human Rights*, NSO Group has a responsibility to respect human rights, including by conducting human rights due diligence to identify, prevent, mitigate and account for its response to human rights risks and impacts.[24] By failing to investigate – or turning a blind

[23] Regarding the importance of the digital space to the formation and holding of opinions by human rights defenders and others, see Report to the Human Rights Council, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, UN Doc. A/HRC/29/32 (2015), paras 20-21, www.undocs.org/A/HRC/29/32 ("Individuals regularly hold opinions digitally, saving their views and their search and browse histories, for instance, on hard drives, in the cloud, and in e-mail archives, which private and public authorities often retain for lengthy if not indefinite periods. Civil society organizations likewise prepare and store digitally memoranda, papers and publications, all of which involve the creation and holding of opinions. . . . Targeted digital interference harasses individuals and civil society organizations for the opinions they hold in many formats. . . . Surveillance systems, both targeted and mass, may undermine the right to form an opinion, as the fear of unwilling disclosure of online activity . . . likely deters individuals from accessing information . . . .").

[24] Report to the Human Rights Council, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, Special Representative of the Secretary General on the

eye to – evidence of human rights violations committed using its products, and continuing to sell its products to regimes known to repress human rights defenders, NSO Group is not fulfilling its responsibility. Despite the foreseeability of the Pegasus spyware platform's misuse when sold to governments with known histories of violating the rights of civil society—and even following public reports that NSO Group's surveillance tools have been used to target journalists, human rights defenders, and political dissidents—there is no evidence that NSO Group has sought to recall its products, perform additional due diligence, or undertake other corrective measures to halt and prevent their further unlawful use.

41. Despite the foreseeable risk of violations of the human rights to privacy, freedom of opinion and expression of human rights defenders resulting from the sale to and use by certain governments of NSO Group's technology, Israel is failing to prevent or restrict such sales. The Israeli government is therefore breaching its duty under international human rights law to protect against violations of rights guaranteed by the ICCPR.[25] Additionally, the *UN Guiding Principles on Business and Human Rights* establish that states "should set out clearly the expectation that all business enterprises domiciled in

issue of human rights and transnational corporations and other business enterprises, John Ruggie, UN Doc. A/HRC/17/31 (2011), Principles 17-21, www.undocs.org/A/HRC/17/31

[25] *See* Human Rights Committee, General Comment 36, Article 6 of the International Covenant on Civil and Political Rights, on the right to life, UN Doc. CCPR/C/GC/36 (2018), para. 63, https://tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/1_Global/CCPR_C_GC_36_8785_E.pdf (recognizing application of Covenant obligations with respect to "persons located outside any territory effectively controlled by the State" who are impacted by state actions "in a direct and reasonably foreseeable manner"); *see also* Human Rights Committee, General Comment 31, The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, UN Doc. CCPR/C/21/Rev.1/Add.13 (2004), para. 8, www.undocs.org/CCPR/C/21/Rev.1/Add.13; Report to the Human Rights Council, The Role of Prevention in the Promotion and Protection of Human Rights, Office of the UN High Commissioner for Human Rights, UN Doc. A/HRC/30/20 (2015), para. 4, www.undocs.org/A/HRC/30/20

their territory and/or jurisdiction respect human rights throughout their operations."[26] To live up to its obligations, the Israeli government, through DECA or another appropriate entity, must take affirmative steps to screen for and prevent against such risks, including by preventing the sale of Pegasus to states with documented records of abusing the rights of human rights defenders.

42. DECA has failed to take any steps to meaningfully protect against harms linked to NSO Group's Pegasus spyware, allowing NSO Group to continue selling its product despite serious allegations of abuse. In November 2018, the Israeli section of Amnesty International sent a letter to DECA requesting the revocation of the defense export license granted to NSO Group that we allege, based on our forensic analysis, was used to target Amnesty International. Because of DECA's inaction, NSO Group can continue to sell its software to governments known to target human rights defenders.
43. Staff of Amnesty International have an ongoing and well-founded fear that they may continue to be targeted and ultimately surveilled through the use of NSO Group's surveillance technology. Without proper oversight by DECA, and adequate due diligence and corrective action by NSO Group to prevent, mitigate, and remedy misuse of its technology, civil society actors remain vulnerable to unlawful surveillance simply for exercising their human rights.

Signature of the submitter

[26] Report to the Human Rights Council, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, Special Representative of the Secretary General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie, UN Doc. A/HRC/17/31 (2011), Principle 2, www.undocs.org/A/HRC/17/31

I hereby certify that on day_____ appeared before an attorney _____ whose office is in _____ Mr. / Ms. _____ that he / she identified himself by ID _____ and after I warned him that he must declare the truth and that he / she will be liable to the penalties prescribed by law, if he / she do not do so, he / she confirm the correctness of the above statement and sign it before me.

_____

The lawyer's stamp and Signature

Exhibit List

[For efficiency, lengthy exhibits attached to the hard copy of this affidavit are excerpted. Full documents are available at the links provided below or for submission at the request of the court.]

1.
    a. Amnesty International, *Amnesty International Among Targets of NSO-powered Campaign*, 1 August 2018, www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign/
    b. Amnesty International, *Amnesty International staff targeted with malicious spyware*, 1 August 2018, www.amnesty.org/en/latest/news/2018/08/staff-targeted-with-malicious-spyware/
2. NSO Group, *Statement*, 17 September 2018, www.citizenlab.ca/wp-content/uploads/2018/09/NSO-Statement-17-September-2018.pdf
3. NSO Group, *Governance & Ethics*, www.nsogroup.com/governance/
4. David D. Kirkpatrick, New York Times, *Israeli Software Helped Saudis Spy on Khashoggi, Lawsuit Says*, 2 December 2018, www.nytimes.com/2018/12/02/world/middleeast/saudi-khashoggi-spyware-israel.html
5. David Ignatius, Washington Post, *How a chilling Saudi cyberwar ensnared Jamal Khashoggi*, 7 December 2018,

www.washingtonpost.com/opinions/global-opinions/how-a-chilling-saudi-cyberwar-ensnared-jamal-khashoggi/2018/12/07/f5f048fe-f975-11e8-8c9a-860ce2a8148f_story.html

6. Josh Rogin, Washington Post, *Washington must wake up to the abuse of software that kills*, 12 December 2018, www.washingtonpost.com/opinions/2018/12/12/washington-must-wake-up-abuse-software-that-kills
7. Chaim Levinson, Haaretz, *Report: Israel Authorized NSO's Sale of Spyware to Saudi Arabia*, 9 December 2018, www.haaretz.com/israel-news/report-israel-authorized-nso-s-sale-of-spyware-to-saudi-arabia-1.6725044
8. Amnesty International, *Meet NSO Group: a go-to company for human rights abusers*, 6 August 2018, www.amnesty.org/en/latest/news/2018/08/is-nso-group-a-goto-company-for-human-rights-abusers/
9. Amos Harel et al, Haaretz, *Revealed: Israeli Cyber Firm Negotiated Advanced Attack Capabilities Sale with Saudis, Haaretz Reveals*, 25 November 2018, www.haaretz.com/israel-news/.premium-israeli-company-negotiated-to-sell-advanced-cybertech-to-the-saudis-1.6680618
10. Toi Staff, Times of Israel, *NSO founder denies its phone hacking software was used to track Khashoggi*, 12 January 2019, www.timesofisrael.com/nso-founder-denies-its-cellphone-hacking-software-used-to-track-khashoggi

11. Shoshanna Solomon, Times of Israel, *NSO founders, management buy stake in firm from Francisco Partners*, 14 February 2019, www.timesofisrael.com/nso-founders-management-buy-stake-in-firm-from-francisco-partners

12. Amnesty International, *Open letter to Novalpina Capital*, 18 February 2019, www.amnesty.org/en/latest/research/2019/02/open-letter-to-novalpina-capital-nso-group-and-francisco-partners/

13. Josh Axelrod, Jerusalem Post, *Report: Israeli Spyware Used to Track Khashoggi Messages, Lawsuit Charges*, 3 December 2018, www.jpost.com/Israel-News/Report-Israeli-spyware-used-to-track-Khashoggi-messages-lawsuit-charges-573419

14. Ronen Bergman, YNetNews.com, *Weaving a cyber web*, 11 January 2019, www.ynetnews.com/articles/0,7340,L-5444998,00.html

15. Bill Marczak et al, Citizen Lab, *Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, 18 September 2018, www.citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

16. Bill Marczak and John Scott-Railton, Citizen Lab, *Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender*, 24 August 2016, www.citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

17. John Scott-Railton et al, Citizen Lab, *Bitter Sweet: Supporters of Mexico's Soda Tax Targeted with NSO Exploit Links*, 11 February 2017, www.citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/

18. John Scott-Railton et al, Citizen Lab, *Reckless VI: Mexican Journalists Investigating Cartels Targeted with NSO Spyware Following Assassination of Colleague*, 27 November 2018, www.citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/

19. Bill Marczak et al, Citizen Lab, *The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil*, 1 October 2018, www.citizenlab.ca/2018/10/the-kingdom-came-to-canada-how-saudi-linked-digital-espionage-reached-canadian-soil/

20. Loveday Morris and Zakaria Zakaria, Washington Post, *Secret recordings give insight into Saudi attempt to silence critics*, 17 October 2018, www.washingtonpost.com/world/secret-recordings-give-insight-into-saudi-attempt-to-silence-critics/2018/10/17/fb333378-ce49-11e8-ad0a-0e01efba3cc1_story.html

21. CBC Radio, *The Current*, 'Activist says Saudi police threatened his family after he tweeted about diplomatic row with Canada', 9 August 2018, www.cbc.ca/radio/thecurrent/the-current-for-august-9-2018-1.4778786/activist-says-saudi-police-threatened-his-family-after-he-tweeted-about-diplomatic-row-with-canada-1.4778820

22. Loveday Morris, Washington Post, *Khashoggi friend sues Israeli firm over hacking he says contributed to the journalist's murder*, 3 December 2018, www.washingtonpost.com/world/middle_east/khashoggi-friend-sues-israeli-firm-over-hacking-he-says-contributed-to-the-journalists-murder/2018/12/03/ddcb28ee-f708-11e8-8642-c9718a256cbd_story.html

23. Siena Anstis, Citizen Lab, *Litigation and Other Formal Complaints Concerning Targeted Digital Surveillance and the Digital Surveillance Industry*, 12 December 2018, www.citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/

24. CBS News, *60 Minutes*, 'CEO of Israeli spyware-maker NSO on fighting terror, Khashoggi murder, and Saudi Arabia', 24 March 2018, www.cbsnews.com/news/interview-with-ceo-of-nso-group-israeli-spyware-maker-on-fighting-terror-khashoggi-murder-and-saudi-arabia-60-minutes/