



July 20, 2022

Mr. Matthew G. Olsen
Assistant Attorney General for National Security
Foreign Agents Registration Act (FARA) Unit
National Security Division
U.S. Department of Justice
175 N Street, NE
Constitution Square, Building 3 - Room 1.300
Washington, DC 20002

Dear Mr. Olsen:

Please accept this letter as a formal report of a violation by four FARA registered agents acting on behalf of the foreign principal, NSO Group (also referred to as N.S.O. Group Technologies Ltd in the FARA database). This information has been researched by DAWN (Democracy for the Arab World Now - www.dawnmena.org), as part of its work to identify and investigate the activities of registered agents on behalf of foreign governments and companies that are violating human rights and engaging in counter-dissident activities.

Pillsbury Winthrop Shaw Pittman LLP, Paul Hastings LLP, Chartwell Strategy Group and Rabinowitz, Inc. (d/b/a Bluelight Strategies) are each FARA registered agents for NSO Group (foreign principal), according to the following registration information:

Foreign Principal

| Name | Registration Date | Registration # (Date) |
|---|--------------------------|------------------------------|
| Pillsbury Winthrop Shaw Pittman LLP | 6/30/2021 | 5198 (7/31/1997) |
| Paul Hastings LLP | 1/24/2022 | 6743 (10/25/2019) |
| Chartwell Strategy Group | 1/12/2022 | 6518 (2/2/2018) |
| Rabinowitz, Inc. (d/b/a Bluelight Strategies) | 3/10/2022 | 7094 (1/22/2021) |

After reviewing the FARA registration forms for these four agents, we have reason to believe that all four provided false information, amounting to a misrepresentation of the foreign principal

(NSO Group). We believe that misrepresentation to be intentional, for the purpose of obscuring the true nature of the company and its business, specifically its control by a foreign government: Israel.

Control by Israel

In the FARA form, “Exhibit A to Registration Statement,” question 10b asks:

If the foreign principal is not a foreign government or a foreign political party:

b) Is this foreign principal:

- Supervised by a foreign government, foreign political party, or other foreign principal
- Owned by a foreign government, foreign political party, or other foreign principal
- Directed by a foreign government, foreign political party, or other foreign principal
- Controlled by a foreign government, foreign political party, or other foreign principal
- Financed by a foreign government, foreign political party, or other foreign principal
- Subsidized in part by a foreign government, foreign political party, or other foreign principal

For each of these questions, all four of the registered agents responded ‘No’ (see links to forms above). This appears to be a coordinated or directed effort to falsify information about NSO Group, which is controlled/directed by a foreign government, Israel.

According to Section 28 CFR § 5.100 (Definition of terms), 12 (b):

As used in the Act, the term *control* or any of its variants shall be deemed to include the possession or the exercise of the power, directly or indirectly, to determine the policies or the activities of a person, whether through the ownership of voting rights, by contract, or otherwise.

Based on the evidence presented below, we maintain that the Israeli government exerts political

control over NSO Group through its “exercise of the power . . . to determine the policies or the activities of a person [NSO Group] . . . by contract,” and that this is confirmed by the public statements of the company, its CEO, and Israeli government officials as reported by the *New York Times* and others articles, some of which cites sources within the company.

Specifically, NSO Group is not able to independently set its own policies or activities in terms of which clients with whom or which it may conduct business; all such contracts are determined by the Government of Israel. Although this may appear to be a normative statutory export control of a regulated technology, the evidence demonstrates that the Government of Israel has, on several occasions, ordered the approval of such exports and decided which clients are approved (and which are not) in order to serve political interests and not to ensure compliance with human rights standards, as the company claims. The above-mentioned evidence, combined with the fact that the NSO Group’s clients are exclusively foreign states and state agencies, leaves little doubt that the Government of Israel’s control over the NSO Group serves political and diplomatic aims, rather than being purely regulatory. It follows then that NSO Group is controlled by the Israeli government per the FARA statute. As such, the four FARA-registered agents should have answered in affirmative in response to the query if the foreign principal is “Controlled by a foreign government, foreign political party, or other foreign principal.”

We acknowledge the term “exercise of power . . . to determine the policies or the activities of a person,” applied to governments, could yield unreasonable results and that a broad interpretation would be counter to the spirit and intent of the statute. However, in this instance, there is substantial evidence that NSO Group’s relationship to the Government of Israel is an exceptional case, and that not enforcing this statute on the foreign principal and its registered agents would undermine the statute itself.

We also maintain that NSO Group should not be considered exempt as outlined in Section 28 CFR § 5.304 Exemptions under sections 3(d) and (e) of the Act. The exemption is only to be allowed “so long as the activities do not directly promote the public or political interests of the foreign government.” Yet, as we document below, by admission of both Israeli government and NSO Group officials, the government is using Pegasus spyware for explicit political purposes to further the interests of the government. Therefore, the activities of the agents of NSO Group are *de facto* promoting the interests of the government of Israel.

The editorial board of *Haaretz*, Israel’s newspaper of record, explained the relationship in an

[editorial](#) titled, “NSO is an Arm of Israel’s Government,” on January 31, 2022. This editorial was published following a *New York Times* [investigation](#), which led *Haaretz* to conclude that “the Netanyahu government traded in export licenses for diplomatic purposes, using Pegasus to win friends, including dictatorships or semi-dictatorships, among them Saudi Arabia.” The *Haaretz* editorial, along with the *New York Times* investigation, depict an exceptional relationship between a government and a seemingly private company.

The four FARA-registered agents have each been registered with FARA prior to their relationship with NSO Group. As such, each agent is familiar with the statute and cannot claim to not have knowledge of the requirements. Furthermore, the abundant public reporting on the NSO Group’s activities and relationship with the Israeli government render any claim by the four agents that they did not have knowledge of the nature of this relationship incredulous. Accordingly, we believe that the FARA Unit should investigate these four lobbyists and their firms and find that their presentation of false information was intentional and intended to mislead the U.S. government, Congress, and the American public.

Evidence

1. Selection of clients as foreign policy of the government

The ability of NSO Group to conduct business is wholly reliant on the Israeli government’s determination of who can be a client of the company. The Israeli government maintains the exclusive ability to decide to whom NSO Group can and cannot sell and, according to credible reports, has in at least one case directed the company not to sell Pegasus spyware to a specific client.

On March 23, 2022, the *Washington Post* [reported](#) that the Israeli government blocked the sale of Pegasus spyware, produced by NSO Group, to the Government of Ukraine. The article states: “The country’s Defense Exports Controls Agency rejected a possible license that would have allowed the NSO Group to offer Pegasus spyware to Ukraine, said the people familiar with the decision, who included Western intelligence officials.” Likewise, the *New York Times* [reported](#):

Even after approving the sale of Pegasus, an Israeli-made spyware program, to dozens of other countries, Israel refused to sell it to Ukraine—rejecting a request last August from

a Ukrainian delegation that visited Israel to discuss spyware purchases, according to an Israeli official and two people familiar with the matter. . . . Israel has instead allowed private Israeli firms to sell Ukrainian military communication equipment and robotics

The specific blocking of Pegasus spyware to Ukraine, while other equipment is approved, demonstrates that the government maintains explicit political control over the company's ability to conduct business and enter into contracts with clients.

Media outlets have regularly reported on the connections between the Israeli government and NSO Group, determining that the government uses the sale of NSO Group software to advance foreign policy interests. As such, the ability to determine which governments can be clients enables the Israeli government to control NSO Group for purposes unrelated to the business interests of the company. For example, on July 17, 2021, the *New York Times* [reported](#):

Israel secretly authorized a group of cyber-surveillance firms to work for the government of Saudi Arabia despite international condemnation of the kingdom's abuse of surveillance software to crush dissent, even after the Saudi killing of the journalist Jamal Khashoggi, government officials and others familiar with the contracts said.

But the Israeli government encouraged NSO and two other companies to continue working with Saudi Arabia, and issued a new license for a fourth to do similar work, overriding any concerns about human rights abuses, according to one senior Israeli official and three people affiliated with the companies.

A response by the Israeli Ministry of Defense to the *New York Times* made it clear that the Israeli government is in a position of control, if not direction, of NSO Group, stating, "The ministry declined to respond to specific questions about the licenses it gave to the Israeli firms, but said that 'a wide range of security, diplomatic and strategic considerations are taken into account' when considering whether to grant a license to export offensive cyber technology."

A subsequent *New York Times Magazine* [investigation](#) into NSO Group and its Pegasus spyware provides seemingly irrefutable evidence of Israeli control. Following the U.S. Department of Commerce sanctioning of NSO Group and adding the company to its Entities List, Israeli officials were outraged.

But Israel also had its own interests to protect. To an extent not previously understood,

Israel, through its internal export-licensing process, has ultimate say over who NSO can sell its spyware to. This has allowed Israel to make NSO a central component of its national-security strategy for years, using it and similar firms to advance the country's interests around the world.

Israeli officials were furious. Many of the headlines focused on the specter of an out-of-control private company, one based in Israel but largely funded offshore. But authorities in Israel reacted as if the ban were an attack on the state itself. 'The people aiming their arrows against NSO,' said Yigal Unna, director general of the Israel National Cyber Directorate until Jan. 5, 'are actually aiming at the blue and white flag hanging behind it.'

The article goes on to detail how, from the very beginning of the company's operations, the government saw the company as a tool for its foreign policy. Mexico was one of the earliest clients of NSO Group, ostensibly to use the spyware to target narcotic trafficking groups. However, Mexico proved to be one of the [earliest examples](#) of how Pegasus spyware was deployed against perceived political opponents—including the media and human rights defenders. Mexican government positions toward Israel began to change following the contract with NSO Group, including a commitment to vote in favor of Israel in resolutions introduced at the United Nations, and reciprocal visits by Israel by Mexican President Enrique Peña Nieto, the first by a Mexican president since 2000, and by Israeli Prime Minister Netanyahu to Mexico, the first ever by an Israeli prime minister.

Even more consequential, however, is what the investigation found regarding how the Israeli government used its control over NSO Group's relationship with the Government of Saudi Arabia; Israeli authorities effectively brokered the contract between NSO Group and the Saudi government in 2017:

In 2017, Israeli authorities decided to approve the sale of Pegasus to the kingdom, and in particular to a Saudi security agency under the supervision of [Crown] Prince Mohammed [bin Salman]. From this point on, a small group of senior members of the Israeli defense establishment, reporting directly to Netanyahu, took a lead role in the exchanges with the Saudis, all 'while taking extreme measures of secrecy,' according to one of the Israelis involved in the affair. One Israeli official said that the hope was to gain Prince Mohammed's commitment and gratitude. The contract, for an initial installation fee of \$55 million, was signed in 2017.

In 2018, Saudi agents acting at the instruction of Crown Prince Mohamed bin Salman murdered U.S. resident, DAWN founder, and *Washington Post* columnist Jamal Khashoggi in the Saudi Consulate in Istanbul. It was widely reported that the Saudi authorities used Pegasus spyware to track the journalist. NSO Group thereafter moved to terminate the contract with the Saudi government. However, in 2019, even as evidence mounted that Saudi Crown Prince Mohammad bin Salman had personally ordered the killing, NSO Group restored the contract with the Saudi government. According to the *New York Times* report, “Keeping the Saudis happy was important for [Prime Minister] Netanyahu, who was in the middle of a secret diplomatic initiative he believed would cement his legacy as a statesman—an official rapprochement between Israel and several Arab states.”

Just a couple of months later, the Saudi license expired, and required renewal by the Israeli Ministry of Defense, which it refused to do. The Crown Prince contacted the Israeli Prime Minister, and the issue was quickly resolved, as reported by the *New York Times*: “Netanyahu apparently had not been updated on the brewing crisis, but after the conversation with Prince Mohammed his office immediately ordered the Defense Ministry to have the problem fixed.”

The Israeli government renewed the Saudi license.

On April 18, 2022, *The New Yorker* [published its own investigation](#) into NSO Group, revealing new information about the targeting of political figures in Europe. The article cited former NSO Group employees, current and former Israeli government officials, and the leadership of NSO Group itself. According to a former NSO Group employee, confirming other reporting, the Israeli government “was well aware of the misuse, and even using it as part of its own diplomatic relationships.” The article goes on to detail how, following the announcement of the Commerce Department sanctions, the CEO of NSO Group, Shalev Hulio, reached out to the Israeli Prime Minister and Defense Minister to intervene with the Americans. Hulio said that he communicated to the Israeli leaders that, “as a regulated company, you know, everything that we have ever asked was with the permission, and with the authority, of the government of Israel.”

2. NSO Group filing in U.S. Supreme Court in WhatsApp case

In 2019, WhatsApp sued NSO Group in a federal district court in California, alleging that the Israeli company had hacked a WhatsApp server to implant Pegasus spyware on over 1,000 personal electronic devices worldwide. NSO Group filed a motion to dismiss the lawsuit,

claiming foreign sovereign immunity. The claim itself would seem to strongly indicate that the company is controlled, directed by, or at the very least regularly avails itself to the direction or control of, a government.

In [seeking a dismissal](#), NSO Group “asserted that the court lacked subject matter jurisdiction because NSO was acting at the direction of its foreign government customers and is protected from suit under foreign sovereign immunity.” While both a Federal District Court and the United States Court of Appeals for the Ninth Circuit rejected NSO Group’s claim of immunity, neither disputed the veracity of NSO Group’s argument that it was being directed by governments (clients). According to *Associated Press* reporting on NSO Group’s appeal, the company argued, “Many nations, including the United States, rely on private contractors to conduct or support core governmental activities. If such contractors can never seek immunity . . . then the United States and other countries may soon find their military and intelligence operations disrupted by lawsuits against their agents.”

3. NSO Group’s Transparency Report

In its [Transparency and Responsibility Report 2021](#), NSO Group acknowledges the control that the Israeli government maintains over the company. On page four of the report, it states: “NSO Group is closely regulated by export control authorities in the countries from which we export our products: Israel, Bulgaria and Cyprus. The Defense Export Controls Agency (DECA) of the Israeli Ministry of Defense strictly restricts the licensing of some of our products . . .”

While many defense and arms exporters are subject to similar licensing arrangements, a significant and credible body of investigative and news reporting over the years indicates that the relationship between NSO Group and the Israeli government is not only regulatory.

The *New York Times* investigation details how NSO Group voluntarily offered to be regulated by Israel’s Ministry of Defense, seemingly to ensure the value of the company to the Israeli government:

The decisions NSO made early on about its relationship with regulators ensured that it would function as a close ally, if not an arm, of Israeli foreign policy . . . When he informed the Defense Ministry that NSO would voluntarily be subject to oversight, the authorities also seemed happy with this plan. One former military aide to Benjamin

Netanyahu, at the time Israel's prime minister, explained the advantages quite clearly. 'With our Defense Ministry sitting at the controls of how these systems move around,' he said, 'we will be able to exploit them and reap diplomatic profits.'

Thus, the promotion of the regulatory framework by NSO Group must be viewed as a means to dissuade further questioning or investigation about the relationship between the Israeli government and the company.

4. Documentation Produced by the FARA-Registered Agents

In multiple documents produced by registered agents (lobbyists) acting on behalf of NSO Group (the foreign principal), the description of the relationship between NSO Group and the Israeli government leaves no doubt that the government maintains control/direction over the business of the company.

On January 10, 2022, Mr. Brian E. Finch, Partner at Pillsbury Winthrop Shaw Pittman, LLP (Pillsbury) and a registered agent for NSO Group, sent a [letter](#) to Congressman Tom Malinowski. The letter provided information about the company in response to Representative Malinowski signing on to a [letter](#) to U.S. Secretary of the Treasury Janet Yellen and U.S. Secretary of State Antony Blinken that requested the application of the Global Magnitsky Act on NSO Group and three other cybersurveillance companies. In explaining NSO Group, Mr. Finch wrote, "We believe that NSO's tools – which are licensed by the Israeli Ministry of Defense under American ITAR-modeled export control regulations and are exclusively operated by the customer – are in fact a force for good in the world."

According to The Electronic Code of Federal Regulations, the basis for the International Traffic in Arms Regulations (ITAR) is the Arms Export Control Act (AECA). Accordingly, "Section 38 of the Arms Export Control Act (22 U.S.C. 2778), as amended, authorizes the President to *control* the export and import of defense articles and defense services."

This open acknowledgement of Israeli control is also evident in a second [document](#) distributed by Pillsbury (filed on January 7, 2022 with FARA), which states, "All sales of NSO Group's technologies are subject to approval by the Israeli government . . ."

On January 7, 2022, Mr. Timothy Dickinson, Senior Counsel at Paul Hastings LLP and FARA-registered agent for NSO Group, sent a [letter](#) to Lisa Peterson, Acting Assistant Secretary, Bureau of Democracy, Human Rights, and Labor at the U.S. Department of State. Mr. Dickinson described the Israeli government-NSO Group relationship as: follows: "NSO is regulated and subject to Israel's stringent export licensing requirements."

In its [contract](#) with NSO Group, Bluelight Strategies seemed to be aware of the ties to the government of Israel when it included a "Legal Compliance" section (which does not appear in

the contracts of the other registrants), stipulating, “Client [NSO Group] represents and warrants that it shall provide truthful information to Bluelight concerning Client, Client’s owners and managers, Client’s ties to or arrangements with the State of Israel; and other topics which may be required to be disclosed by Bluelight pursuant to applicable law.”

Despite this provision, Bluelight, like the other three registrants, checked the ‘no’ boxes in response to the question about foreign government control when completing the FARA registration forms.

Conclusion

From the available evidence, including credible and detailed media reporting, court filings, and information the company and its lobbyists promote about NSO Group, it is clear that NSO Group is controlled and/or directed by the Israeli government and possibly also its foreign government clients (according to NSO Group’s claims in the WhatsApp lawsuit). The fact that four separate lobbying firms that registered as FARA agents on behalf of NSO Group each misrepresented the true nature of the company suggests that this was not accidental or an oversight, but rather a coordinated or directed effort to mislead the FARA Unit, the Department of Justice, and the American people.

As is well documented, the purpose of FARA is to ensure transparency with regard to lobbying on behalf of foreign actors. In this case, the misrepresentation of a company that has been [sanctioned](#) by the U.S. Department of Commerce, and that has been widely reported to have enabled repressive and authoritarian governments, is of acute concern and a matter of national security. We request the FARA Unit to immediately investigate these concerns and, if the violations as reported here are found to be true, to impose criminal penalties on each of the firms, per the terms outlined in [22 U.S.C. § 618\(a\)](#). Action in this case would set a strong example for firms lobbying on behalf of technology companies where there is close cooperation with a state, while inaction would suggest that FARA registration can be treated as a mere box-ticking exercise without standards or consequences.

We appreciate your time and consideration of this complaint and we look forward to hearing from you.

Sincerely,



Adam Shapiro
Director of Advocacy, Israel/Palestine
ashapiro@dawnmena.org