IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

HANAN ELATR KHASHOGGI, Plaintiff, v. NSO GROUP TECHNOLOGIES LIMITED and Q CYBER TECHNOLOGIES LIMITED, Defendants.	)	1:23-cv-779 (LMB/LRV)

MEMORANDUM OPINION

This civil action arises out of the brutal assassination of journalist and human rights activist Jamal Khashoggi in the Saudi Arabian consulate in Istanbul, Turkey. On June 15, 2023, his wife, plaintiff Hanan Elatr Khashoggi ("plaintiff" or "Hanan")[1] filed a seven-count Complaint in which she alleges that for nearly a year leading up to her husband's October 2, 2018 murder, her phones had been infiltrated by spyware designed, sold, and maintained by defendants NSO Group Technologies Limited ("NSO Group") and Q Cyber Technologies Limited ("Q Cyber") (collectively, "defendants" or "NSO Group"). The spyware allegedly was used by agents of the governments of the Kingdom of Saudi Arabia ("Saudi Arabia") and the United Arab Emirates ("UAE") to obtain information from two of plaintiff's phones that was then used to carry out the surveillance and assassination of her husband.

Before the Court is defendants' Motion to Dismiss the Complaint ("Motion to Dismiss") for lack of jurisdiction and for failure to state a claim upon which relief can be granted. [Dkt. No. 23]. Defendants' Motion to Dismiss is fully briefed and oral argument has been held. For the reasons that follow, defendants' Motion to Dismiss will be granted.

[1] In the Complaint, plaintiff is primarily referred to as "Hanan."

I. BACKGROUND

A. Procedural History

In her Complaint, plaintiff alleges seven causes of action against defendants: violation of the federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030 et seq. (Count I); violation of the Virginia Computer Crimes Act, Va. Code § 18.2-152.1 et seq. (Count II); negligence (Count III); trespass to chattels (Count IV); intentional infliction of emotional distress (Count V); negligent infliction of emotional distress (Count VI); and a demand for equitable relief to identify defendants' clients and agents (Count VII). [Dkt. No. 1] at ¶¶ 134-193. Defendants' Motion to Dismiss offers six arguments to support dismissal of plaintiff's Complaint: 1) derivative foreign sovereign immunity and lack of subject-matter jurisdiction; 2) lack of personal jurisdiction; 3) the act of state doctrine; 4) forum non conveniens; 5) extraterritorial application of state law; and 6) failure to state a claim upon which relief can be granted under Fed. R. Civ. P. 12(b)(6). See [Dkt. No. 26]. Because defendants have satisfactorily demonstrated that the alleged facts and governing law support their position with respect to subject-matter and personal jurisdiction, their Motion to Dismiss will be granted, and the Court will not address defendants' act of state, forum non conveniens, and Rule 12(b)(6) arguments.[2]

B. Factual Allegations

According to the Complaint, plaintiff is a citizen of Egypt and a lawful resident of the United States currently seeking political asylum. [Dkt. No. 1] at ¶¶ 6-7. She is the widow of Jamal Khashoggi, a "writer, editor, and activist who was well-known for his thoughtful opinions on the rights of women and other minorities, and his calls for governmental reform in Saudi

[2] Despite resolving the Motion to Dismiss on jurisdictional grounds alone, the Court recognizes that defendants posit strong arguments that a more appropriate forum for this civil action would be in Israel and plaintiff likely fails to state claims upon which relief can be granted.

Arabia and the Middle East." Id. at ¶ 8. Plaintiff is legally employed through a work visa and lives full-time in Virginia. Id. at ¶ 9.

Defendant NSO Group is a limited liability company incorporated in Israel, which "create[s], develop[s], [sells], and assist[s] in the deployment and use of cutting-edge spyware technology to clients around the world." Id. at ¶ 20. NSO Group is a subsidiary of defendant Q Cyber, a private company also incorporated in Israel. Id. at ¶¶ 21-22.[3] Plaintiff alleges that NSO Group "has been primarily funded and controlled by California-based investment funds and . . . has a U.S. subsidiary company, Westbridge Technologies, Inc. ("Westbridge"), that is headquartered in Virginia." Id. at ¶ 30.[4]

The spyware alleged to have aided in the collection of information that ultimately led to the assassination of Jamal Khashoggi is known as "Pegasus," which the Complaint describes as "an advanced surveillance tool designed to be undetectable—it evades traditional security measures and it is installed on the user's device without their knowledge or consent." [Dkt. No. 1] at ¶ 40. While Pegasus can remotely infect a target's cell phone using only a simple text message, it also has a remote "zero click" feature which enables a phone to be compromised even where there has been no interaction by its user. Id. at ¶ 41. Instead, a party employing Pegasus need only target the phone number in order to see "every piece of data stored on the

[3] Plaintiff alleges that NSO Group and Q Cyber are managed, in all respects, by one of the companies' founders, Omri Lavie. [Dkt. No. 1] at ¶¶ 23-25.

[4] NSO is alleged to have created Westbridge to help sell its spyware to the United States market, [Dkt. No. 1] at ¶ 30; however, plaintiff does not allege that Westbridge had any involvement in the conduct underlying this civil action. Defendants argue that Westbridge is not actually a subsidiary of NSO Group but a "corporate affiliate owned by the same ultimate parent company" as NSO Group. [Dkt. No. 48] at 4 n.4.

phone."[5] Installation of the spyware can be done using various remote "installation vectors," including remote installation "over-the-air" ("OTA") or through Enhanced Social Engineering Messages ("ESEM"). Id. at ¶ 49.[6]

In the cyber security context, "social engineering" refers to a manipulative tactic to induce the target to provide their own vulnerabilities to a bad actor. This is commonly referred to as "phishing," where a website, email, or text message appears to be legitimate, but in fact induces the target to click on a link that exposes the device to malware or spyware. Quoting from NSO Group's alleged "sales brochure," the Complaint describes Pegasus as providing "a wide range of tools to compose a tailored and innocent message to lure the target to open the message." Id. at ¶ 52 (quoting Ex. 1 at 13). These phishing messages are designed to be sent either to a primary or direct target or to a "relational" or "off-center" target, usually a spouse, sibling, parent, staff member, or close associate of the primary target. Id. at ¶ 54 (citations omitted). According to the Complaint, infiltrating the device of a relational target allows "NSO Group's clients to circumvent the security features that are typically utilized by hyper-vigilant primary targets, like Jamal Khashoggi." Id. at ¶ 54 (citations omitted).[7]

The Complaint alleges three technical ways for NSO Group's clients to gain total control of a device using Pegasus: "(1) remote, zero-click entry via software exploit; (2) physical

---

[5] See [Dkt. No. 1] at ¶ 41; see also Ronen Bergman & Mark Mazzetti, "The Battle for the World's Most Powerful Cyberweapon," N.Y. TIMES (Jan. 28, 2022), https://www.nytimes.com /2022/01/28/magazine/nsogroup-israel-spyware.html.

[6] Plaintiff has attached to her Complaint as Exhibit 1 a purported Pegasus "sales brochure" allegedly created by NSO Group. See generally [Dkt. No. 1] Ex. 1.

[7] NSO Group publicly contends that it can identify and stop any "misuse" of Pegasus, such as the targeting of activists' family members; however, plaintiff alleges that NSO Group has failed to do so, "as evidenced by the number of times Pegasus has been used to spy on innocent individuals." [Dkt. No. 1] at ¶ 60 (citing examples).

installation on the device; and/or (3) inducing the target to unwittingly install Pegasus on their device via ESEM. To maximize the chance of successful infiltration, clients can utilize one or more of these methods." [Dkt. No. 1] at ¶ 65.

The Complaint alleges that NSO Group has sold its Pegasus software or other spyware to the governments of Ghana, Rwanda, the United Arab Emirates, and Saudi Arabia, among others, id. at ¶ 39 n.6, and works to analyze data on behalf of clients and generates reports based on the data obtained from targets' devices, id. at ¶ 46; see also [Dkt. No. 45] at 1-2 ("NSO [Group] configures and maintains the infrastructure that supports the operation of Pegasus, trains clients in its use, and assists those clients throughout every stage of the deployment and operation of the spyware.").

Although the Complaint provides extensive details about the events that gave rise to the assassination of Jamal Khashoggi, the only allegations relevant to resolving defendants' Motion to Dismiss are the following:

- "[I]n November 2017, the first Pegasus attempts were made on one of Hanan's cell phones, just as she was growing closer with Jamal. These were ESEM text messages that were personalized to induce her to follow the malicious link containing Pegasus." Id. at ¶ 101.

- "[A]t 06:46:59 GMT on November 26, 2017, Hanan received a text message stating that a flower bouquet was sent to her. She later clicked and followed the link and was rerouted to a disabled Pegasus link. Citizen Lab attributed the domain name in these links to an agency of the UAE." Id. at ¶ 102.

- "At least five more attempts were made via ESEM text messages sent to Hanan's phone in November 2017." Id. at ¶ 103.

- "In April 2018, while working as a flight attendant, Hanan arrived at the Dubai International Airport and found seven Emirati intelligence officers waiting for her. Hanan was blindfolded, handcuffed, and transported to a remote interrogation cell where she was questioned about Jamal and his activities for over 17 hours. Hanan was detained and her captors took both of her cell phones that

she had been using to communicate with Jamal. Citizen Lab later confirmed in its analysis that it was likely during this time that Pegasus was manually installed onto at least one of her phones." Id. at ¶ 106.[8]

- "Hanan was placed under house arrest in the UAE until May 2018, when she returned to the United States to be with Jamal." Id. at ¶ 107.

- "On June 2, 2018, Hanan and Jamal were married . . . in Alexandria, VA. . . . They spent the next weeks moving into and decorating their shared apartment in Virginia and making it her home." Id. at ¶ 110.

- "When the two were forced to be apart, they were in frequent contact through text messages, WhatsApp, phone calls, and various other apps Jamal insisted they use for privacy. Unfortunately, Jamal's suspicions were well-founded, but use of multiple apps or frequently changing SIM cards was no match for NSO Group's technology. Neither suspected that Hanan herself might become a target." Id. at ¶ 111.

- "Upon information and belief, all of Jamal and Hanan's conversations—by phone, message, or in person—were available to NSO Group and ultimately relayed to the Saudis, via the UAE, providing key information and proof of Jamal's persistent belief that Saudi Arabia needed reform." Id. at ¶ 113.

See generally [Dkt. No. 1] at ¶¶ 101-13.

On October 2, 2018, Jamal Khashoggi disappeared after visiting the Saudi consulate in Istanbul. The United States Office of the Director of National Intelligence released a report concluding that "Saudi Arabia's Crown Prince Muhammad bin Salman approved an operation in Istanbul, Turkey to capture or kill Saudi journalist Jamal Khashoggi."[9]

---

[8] The Complaint alleges that "the Kingdom of Saudi Arabia had leveraged its relationship with a key ally, the United Arab Emirates, to install Pegasus on [plaintiff's] phones, which would then allow [Crown Prince Muhammad bin Salman] to monitor and track Jamal." [Dkt. No. 1] at ¶ 108 n.55.

[9] See Assessing the Saudi Government's Role in the Killing of Jamal Khashoggi (Feb. 11, 2021), https://www.dni.gov/files/ODNI/documents/assessments/Assessment-Saudi-Gov-Role-in-JK-Death-20210226v2.pdf.

Nearly three years later, a forensic investigation performed by Citizen Lab, a research laboratory based out of the University of Toronto's Munk School of Global Affairs, provided evidence that both of plaintiff's Android phones were infected with Pegasus by April 2018, "and likely earlier, with attempts on her devices dating back to November 2017." [Dkt. No. 1] at ¶ 42.

> The infiltration allowed for all information stored on Plaintiff's phones to become accessible. However, it also granted access to all future phone calls, communication activity through apps, and text messages in perpetuity. Further, the infiltration gave NSO [Group] and [its] client(s) the ability to activate the cameras and microphones of Plaintiff's phones without her knowledge, turning her phones into sophisticated listening and recording devices.

Id. Citizen Lab found evidence that the Pegasus software was likely installed via physical installation on plaintiff's phones while she was in the Dubai airport in April 2018 and that she received a number of malicious ESEM texts containing links that would also install Pegasus on her phones in 2017. Id. at ¶ 65. Neither the Complaint nor the Citizen Lab report detailed the location of either plaintiff or the devices when the messages were received or opened.

II. DISCUSSION

Defendants argue that the Complaint should be dismissed under Rules 12(b)(1) and 12(b)(2) for lack of jurisdiction, in addition to arguments asserting the act of state doctrine, forum non conveniens, extraterritoriality, and failure to state a claim under Rule 12(b)(6). As previously mentioned, the Court will address only the jurisdictional arguments and grant the Motion to Dismiss with prejudice.

A. Standard of Review

Under Rule 12(b)(1) of the Federal Rules of Civil Procedure, an action must be dismissed if the court lacks subject-matter jurisdiction. The plaintiff, as the party asserting jurisdiction, bears the ultimate burden of proving such jurisdiction. Adams v. Bain, 697 F.2d 1213, 1219 (4th Cir. 1982). If "a complaint simply fails to allege facts upon which subject matter jurisdiction can

be based[,] . . . all the facts alleged in the complaint are assumed to be true and the plaintiff, in effect, is afforded the same procedural protection as he would receive under a Rule 12(b)(6) consideration." Id. But in the event of a factual dispute over the jurisdictional allegations in the complaint, the court may consider evidence outside the complaint "without converting the proceeding to one for summary judgment." Id.

Moreover, a federal court may dismiss an action under Federal Rule of Civil Procedure 12(b)(2) for lack of personal jurisdiction. A plaintiff need only make a "prima facie showing of a sufficient jurisdictional basis," and "the court must construe all relevant allegations in the light most favorable to the plaintiff and draw the most favorable inferences for the existence of jurisdiction." Verizon Online Servs., Inc. v. Ralsky, 203 F. Supp. 2d 601, 609 (E.D. Va. 2002) (citing Combs v. Bakker, 886 F.2d 673, 676 (4th Cir. 1989)).

B. Analysis

1. Derivative Foreign Sovereign Immunity

In their Motion to Dismiss, defendants first contend that the Court lacks subject-matter jurisdiction to consider plaintiff's claims because they represent an attempted end-run around the foreign sovereign immunity of Saudi Arabia and the UAE. [Dkt. No. 23] at 6-7. The Foreign Sovereign Immunities Act ("FSIA") deprives federal courts of jurisdiction over claims brought against a foreign state. See 28 U.S.C. § 1604 ("[A] foreign state shall be immune from the jurisdiction of the courts of the United States and of the States . . . ."). Specifically, defendants argue that the Court lacks subject-matter jurisdiction over plaintiff's claims because all of NSO Group's alleged actions at issue in this civil action were taken on behalf of Saudi Arabia and the UAE. [Dkt. No. 23] at 7. Defendants concede that they are not covered by the express text of the FSIA, which immunizes only foreign states, not private companies; however, they contend that they are entitled to "common-law foreign sovereign immunity," id., which is extended "to

an individual acting in his official capacity on behalf of a foreign state," Velasco v. Gov't of Indonesia, 370 F.3d 398, 399 (4th Cir. 2004). Defendants' argument fails in two respects.

First, the FSIA governs all foreign sovereign immunity claims brought by private entities. See WhatsApp Inc. v. NSO Group Techs. Ltd., 17 F.4th 930, 940 (9th Cir. 2021) (differentiating the FSIA's application between "entities" and "individuals"). NSO Group's attempt to refashion itself as an individual—and not an entity—is unavailing. NSO Group is a private corporation that designs spyware technology used by governments for law enforcement purposes. Second, it is clear that NSO Group cannot meet the FSIA's definition of "foreign state," because it is neither a foreign sovereign, 28 U.S.C. § 1603(a), nor "an organ . . . or political subdivision" of a foreign sovereign. Id. § 1603(b)(2). Instead, NSO Group is a private corporation that provides products and services to sovereigns. No matter the use to which its customers put NSO Group's technology, its services do not render it an "agency or instrumentality of a foreign state," as Congress has defined that term in the FSIA. For these reasons, defendants are not entitled to the protection of foreign sovereign immunity under the FSIA.

This conclusion is supported by a decision of the U.S. Court of Appeals for the Ninth Circuit which held the same when it squarely rejected NSO Group's claim of derivative common law foreign sovereign immunity.

> There is no need to analyze whether NSO [Group] is entitled to immunity under the common law and inquire how the State Department would resolve this case. See WhatsApp Inc. v. NSO Grp. Techs. Ltd., 472 F. Supp. 3d 649, 665 (N.D. Cal. 2020). Nor is it necessary to explain that neither the State Department nor any court has ever applied foreign official immunity to a foreign private corporation under the common law, although this is a compelling fact indeed. The proper analysis begins and ends with the FSIA, the comprehensive framework Congress enacted for resolving any entity's claim of foreign sovereign immunity.

WhatsApp, 17 F.4th at 940 (cleaned up). Since the FSIA is the sole source for NSO Group's purported immunity claim, and the FSIA does not reach the commercial conduct of privately-owned companies, NSO Group lacks a foundation on which to assert a derivative sovereign immunity claim.

Despite this door being closed, NSO Group points to several cases addressing the derivative immunity of foreign government "officials." See [Dkt. No. 23] at 7 (citing Velasco, 370 F.3d at 399; Yousuf v. Samantar, 699 F.3d 763, 769 (4th Cir. 2012); Doğan v. Barak, 932 F.3d 888, 893-94 (9th Cir. 2019); Rishikof v. Mortada, 70 F. Supp. 3d 8, 13 (D.D.C. 2014); Herbage v. Meese, 747 F. Supp. 60, 66 (D.D.C. 1990); Butters v. Vance Int'l, Inc., 225 F.3d 462, 466 (4th Cir. 2000)). None support NSO Group's argument.

NSO Group bases its argument primarily on Butters v. Vance International, Inc., in which a United States-based employee sued her employer, a United States corporation. Id. at 464. The employer provided "security services to corporations and foreign sovereigns," specifically to the wife of the king of Saudi Arabia while she was undergoing medical treatment in California. Id. The employee was hired to provide security services but, because of the religious beliefs of the visiting Saudi officials, was not permitted to work in the command post and eventually filed a gender discrimination suit against her employer. Id.

The Fourth Circuit determined that the United States company could assert derivative sovereign immunity. Id. at 466. The court relied on Yearsley v. W.A. Ross Construction Co., 309 U.S. 18, 21-22 (1940), for the proposition that "contractors and common law agents acting within the scope of their employment for the United States have derivative sovereign immunity." Butters, 225 F.3d at 466. The Fourth Circuit then extended the rule of derivative sovereign immunity to American private agents of foreign governments:

> It is but a small step to extend this privilege to the private agents of foreign governments. All sovereigns need flexibility to hire private agents to aid them in conducting their governmental functions. This is especially true for foreign sovereigns given their lack of human resources while operating within the United States. To abrogate immunity would discourage American companies from entering lawful agreements with foreign governments and from respecting their wishes even as to sovereign acts.

Butters, 225 F.3d at 466. NSO Group likens this civil action to Butters; in that, plaintiff alleges that the UAE monitored her devices on behalf of Saudi Arabia and did so using NSO Group's technology, and a "foreign government's deployment of clandestine agents to collect foreign intelligence . . . is peculiarly sovereign conduct." [Dkt. No. 23] at 7-8 (cleaned up).

NSO Group's argument, including its analogy to the holding of Butters, comes up short. First, in Butters, the Fourth Circuit extended the doctrine of "domestic derivative sovereign immunity," applicable to United States contractors, to a United States corporation acting as an agent of a foreign sovereign while in the territorial United States. Butters, 255 F.3d at 466. In that case, the defendant asserting derivative sovereign immunity was a United States corporation and the Fourth Circuit's reasoning indicated that the United States citizenship of the company was necessary to its holding. See Butters, 225 F.3d at 466 ("To abrogate immunity would discourage American companies from entering lawful agreements with foreign governments and from respecting their wishes even as to sovereign acts."). None of the other cases cited by NSO Group involve the application of derivative sovereign immunity to foreign entities. And Butters did not reach whether this purported common-law doctrine also extends to foreign contractors acting on behalf of foreign states for alleged conduct that occurred outside of the borders of the United States. Moreover, the holding of Butters was put into question after the United States Supreme Court instructed that "any sort of immunity defense made by a foreign sovereign in an American court must stand on the [FSIA's] text. Or it must fall." Republic of Argentina v.

NML Cap., Ltd., 573 U.S. 134, 142 (2014). Because NSO Group is a private foreign entity that is not entitled to sovereign immunity under the FSIA, the Court will deny defendants' Motion to Dismiss with respect to this argument.

2. Personal Jurisdiction

Although the Court rejects NSO Group's sovereign immunity argument, its argument that plaintiff has failed to plead sufficient facts to support personal jurisdiction in Virginia is meritorious. Plaintiff has the burden to allege plausible facts that indicate a significant connection between NSO Group and its alleged conduct and this forum.

To start, defendants are not subject to general personal jurisdiction in Virginia—a point that plaintiff concedes. As a company incorporated and with its principal place of business in Israel, NSO Group's contacts with Virginia are not "so constant and pervasive to render it essentially at home." Daimler AG v. Bauman, 571 U.S. 117, 122 (2014) (cleaned up). Therefore, this civil action may only proceed if the Court has specific personal jurisdiction over defendants.

The inquiry into whether a forum state may assert specific personal jurisdiction over a nonresident defendant focuses on the relationship among the defendant, the forum, and the litigation. Walden v. Fiore, 571 U.S. 277, 283–84 (2014) (citation omitted). "Federal courts ordinarily follow state law in determining the bounds of their jurisdiction over persons." Daimler, 571 U.S. 117 (2014); see Fed. R. Civ. P. 4(k)(1)(a). Virginia's long-arm statute extends personal jurisdiction over nonresident defendants to the full extent permitted by the Fourteenth Amendment's Due Process Clause. See, e.g., CFA Inst. v. Inst. of Chartered Fin. Analysts of India, 551 F.3d 285, 293 (4th Cir. 2009); Peninsula Cruise, Inc. v. New River Yacht Sales, Inc., 512 S.E. 2d 560 (Va. 1999). "Because Virginia's long-arm statute is intended to

extend personal jurisdiction to the extent permissible under the due process clause," the statutory and constitutional questions merge into one inquiry. Consulting Eng'rs Corp., 561 F.3d 273, 277 (4th Cir. 2009) (citation omitted). Thus, to establish specific personal jurisdiction the Complaint must allege facts showing that plaintiff's claims "arise out of" activities by which NSO Group "purposefully availed itself of the privilege of conducting activities in" Virginia. Carefirst of Md., Inc. v. Carefirst Pregnancy Ctrs., Inc., 334 F.3d 390, 397 (4th Cir. 2003); see also Hanson v. Denckla, 357 U.S. 235, 250-53 (1958); Goodyear Dunlop Tires Operations, S.A. v. Brown, 564 U.S. 915, 924-25 (2011).

To meet the constitutional due process requirements for personal jurisdiction, NSO Group must have "minimum contacts" such that "the maintenance of the suit does not offend traditional notions of fair play and substantial justice." Consulting Eng'rs Corp., 561 F.3d at 277 (quoting Int'l Shoe Co. v. Wash., 326 U.S. 310 (1945)). The minimum contacts inquiry requires plaintiff to allege facts that make a plausible showing that NSO Group "purposefully directed [its] activities at the residents of the forum" and that plaintiff's causes of action "arise out of" those activities. Burger King Corp. v. Rudzewicz, 471 U.S. 462, 472 (1985) (citation and quotation omitted). The inquiry is designed to ensure that a foreign defendant, like NSO Group, is not "haled into a jurisdiction solely as a result of random, fortuitous, or attenuated contacts." Id. at 475. In other words, it protects defendants from having to defend themselves in a forum where they did not anticipate being sued. See World–Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 297 (1980); see also ESAB Group, Inc. v. Centricut, Inc., 126 F.3d 617, 623 (4th Cir. 1997) (underscoring that minimum contacts must have been so substantial that "they amount to a surrogate for presence and thus render the exercise of sovereignty just").

The Fourth Circuit has synthesized the requirements for asserting specific personal jurisdiction into a three-prong test: "(1) the extent to which the defendant purposefully availed itself of the privilege of conducting activities in the State; (2) whether the plaintiffs' claims arise out of those activities directed at the State; and (3) whether the exercise of personal jurisdiction would be constitutionally reasonable." Consulting Eng'rs Corp., 561 F.3d at 278 (quoting ALS Scan, Inc. v. Digital Serv. Consultants, Inc., 293 F.3d 707, 712 (4th Cir. 2002) (quotations and citations omitted)).

a. Purposeful availment

The first prong, purposeful availment, concerns whether and to what extent the defendants purposefully availed themselves of the privilege of conducting activities in Virginia. Carefirst of Md., 334 F.3d 390, 397. The Fourth Circuit has previously held that this prong is not susceptible to a mechanical application. Consulting Eng'r Corp., 561 F.3d at 278. It is necessary to consider how the alleged facts apply to the particular circumstance in which, as here, out-of-state defendants have acted outside of the forum in a manner that allegedly injures someone residing in the forum. In Calder v. Jones, 465 U.S. 783 (1984), the Supreme Court held that a court may exercise specific personal jurisdiction over a nonresident defendant acting outside of the forum when the defendant has intentionally directed his tortious conduct toward the forum state, knowing that its conduct would cause harm to a forum resident. Id. at 789–902.[10] Applying that test to the libel suit before it, the Calder court held that California possessed jurisdiction over Florida reporters who had written an allegedly libelous article for the

[10] In their briefs, the parties base their arguments mainly on Consulting Engineers Corporation; however, that case is more appropriate in the context of a personal jurisdiction inquiry related to a business or contractual dispute. The more appropriate analysis for an alleged intentional tort committed by an out-of-state defendant is Calder.

National Enquirer about a California actress, because "California [was] the focal point both of the story and of the harm suffered." Id. at 789. The writers' "actions were expressly aimed at California," the Court said, "[a]nd they knew that the brunt of [the potentially devastating] injury would be felt by [the actress] in the State in which she lives and works and in which the National Enquirer has its largest circulation." Id. at 789–90; see also ESAB Group, 126 F.3d at 625–26 (emphasizing the importance, in light of Calder, of evidence that defendant expressly aimed or directed its conduct toward forum state and noting that business activities focusing "generally on customers located throughout the United States and Canada without focusing on and targeting" forum state cannot yield personal jurisdiction).

Even though plaintiff asserts that NSO Group "intentionally target[ed] . . . her devices in Virginia," [Dkt. No. 1] at ¶ 30, she does not support that allegation with sufficient, non-conclusory facts or plausible assertions. For example, plaintiff claims that NSO Group created a substantial connection with Virginia and "purposefully direct[ed] surveillance activities towards [plaintiff's] devices while she resided in Virginia." [Dkt. No. 45] at 3. Despite alleging that the surveillance was ongoing in this district, and that NSO Group "and its clients" targeted plaintiff, the Complaint fails to include any non-conclusory allegations regarding how long and where plaintiff had been living in the district, and how NSO Group specifically participated in the surveillance of her phones while she was in Virginia, as opposed to conduct that may have happened while she was overseas or travelling for work as a flight attendant for Emirates Airlines. Nor does the Complaint allege facts that counter defendants' argument that the non-party Saudi and Emirati governments were the ones using the Pegasus technology to surveil plaintiff.

NSO Group is an Israeli corporation, which plaintiff is suing because it licensed its technology to foreign sovereigns that plaintiff alleges used the technology to monitor her devices. The Complaint never pleads with specificity that any of this monitoring occurred while plaintiff was in this forum. Defendants have no offices in Virginia and there are no allegations that they solicit business in Virginia. The Complaint does not allege that NSO Group solicited the business of the Saudi or Emirati governments in Virginia, nor does it allege that defendants made in-person contact with plaintiff in Virginia. Moreover, the only direct contact alleged between NSO Group and Saudi Arabia and the UAE is that NSO Group, with the Israeli government's approval, licensed its technology to those sovereign nations.

The Complaint alleges that an agent of the UAE sent plaintiff a "text message" containing a "disabled Pegasus link" in November 2017, [Dkt. No. 1] at ¶ 102; however, it does not specifically allege that plaintiff was either in Virginia when she received that message or clicked on that link. Instead, the Complaint states that Jamal Khashoggi "invited her to reconnect with him in his new home in Virginia . . . after the summer of 2017." Id. at ¶ 12. When asked in open court about how long plaintiff was living in Virginia, counsel indicated that plaintiff regularly entered and exited the Commonwealth because of her work schedule as a flight attendant, but counsel was unable to link specific dates to specific alleged conduct by NSO Group occurring in Virginia. For example, the alleged manual installation of Pegasus on plaintiff's phones is repeatedly described as occurring in the Dubai airport, not in Virginia. See, e.g., [Dkt. No. 1] at ¶¶ 14, 106. Even if plaintiff could plead sufficient facts supporting a claim that Pegasus was installed on her phones while she was in Virginia, or that Pegasus captured data from her phones while plaintiff was in Virginia, those actions were carried out by third-parties who plaintiff alleges were using Pegasus, not by defendants.

The weakness of plaintiff's argument that the Court has personal jurisdiction over these defendants is demonstrated by the inaccurate way in which plaintiff's briefing cites authorities. To support plaintiff's claim that defendants purposefully availed themselves of this forum, plaintiff cites to UMG Recordings, in which the Fourth Circuit reversed a district court's order granting a motion to dismiss based on a lack of personal jurisdiction. In that case, the defendant was a Russian citizen who resided outside the United States but operated a website that illegally streamed audio tracks from YouTube videos. UMG Recs., Inc. v. Kurbanov, 963 F.3d 344, 348 (4th Cir. 202). The Fourth Circuit found that the defendant's contacts with Virginia were "plentiful," such that the defendant had "fair warning that his forum related activities could subject him to Virginia's jurisdiction." Id. at 353 (cleaned up). Among the evidence in that case was that, in a one-year period, more than half a million unique visitors went to the defendant's website, totaling nearly 1.5 million visits, with Virginia being one of the most popular states in terms of unique visitors as well as the number of visits. Id. The Fourth Circuit also pointed to the defendant's collection of IP addresses and personally-identifying-data from the users who chose to engage with his website as a basis for finding that the defendant personally availed himself of Virginia's jurisdiction. Id.

Moreover, in UMG Recordings, unlike this civil action, the defendant was the direct actor who injured the plaintiff. By contrast, plaintiff's Complaint describes the UAE and Saudi Arabia as the entities that targeted her phones—and ultimately her husband—and collected information from her devices. Plaintiff does not allege that NSO Group knowingly directed or guided Saudi Arabia and the UAE to use Pegasus to monitor plaintiff in Virginia. "[T]he mere act of aiding and abetting is not always enough to provide minimum contacts" because "aiding-and-abetting

. . . does not necessarily involve the sort of 'express aiming' at the forum that the effects test requires." Hawkins v. i-TV Digitalis Tavkozlesi zrt., 935 F.3d 211, 230-31 (4th Cir. 2019).

Next, plaintiff cites to Verizon Online Services v. Ralsky, which involved the transmission of millions of unsolicited bulk e-mail ("UBE" or "spam") passing through seven of Verizon's Virginia servers to Verizon's subscribers through its proprietary on-line network. The court found these contacts with Virginia were sufficient to support specific personal jurisdiction over the foreign defendant in Virginia. The facts in that case demonstrate how significantly plaintiff's allegations fail. In Verizon Online Services, the defendants themselves engaged directly in constructing thousands of spam messages and transmitted them to customers via servers located in Virginia. As the court found, "Defendants solicited business from Verizon's subscribers for pecuniary gain, while at the same time trespassing on Verizon's proprietary network causing harm to its servers located in Virginia." 203 F. Supp. 2d 601, 604 (E.D. Va. 2002). Ultimately, the court found that allowing defendants to "escape personal jurisdiction in a forum they have exploited for pecuniary gain while causing a tort to a Virginia resident would constitute a manifest unfairness to the rights of Verizon and the interests of Virginia." Id. Once again, the defendants in that case were the direct actors, rather than, at best, aiders and abettors.

At oral argument, plaintiff's counsel repeatedly characterized plaintiff's claims as ones leaving open the "possibility" that NSO Group purposefully targeted plaintiff while she was in Virginia. But, as defense counsel responded, "possibility" is precisely the wrong standard. The Complaint must make plausible allegations that NSO Group purposefully aimed its conduct at

plaintiff in Virginia. Plaintiff does not plausibly allege any specific Virginia-related conduct by NSO Group.[11]

b. Claims arising out of conduct in Virginia

The second prong, whether plaintiff's claims arise out of the activities directed at the forum, concerns to what extent NSO Group's contacts with Virginia form the basis of the suit, i.e., the federal Computer Fraud and Abuse Act and state claims. Consulting Eng'g, 561 F.3d at 278–79 (citations omitted). Here, defendants contend that the limited conduct plaintiff attributes to them has no connection to Virginia and that they took no action to subject themselves to suit in the Commonwealth.

The Complaint alleges that NSO Group "utilized . . . [plaintiff's] personal devices" on an ongoing basis and "caused tortious injury to [plaintiff] in Virginia when they infiltrated and continuously monitored [her] through her devices." [Dkt. No. 1] at ¶¶ 36-42. The Complaint continues, claiming "NSO Group laid every intimate detail of her life bare," including her messages, medical and financial information, and private conversations in her Virginia home. Id. at ¶ 47. Plaintiff's theory as to who and how this conduct was committed is somewhat opaque. For example, plaintiff alleges that NSO Group "configures and maintains the infrastructure that supports the operation of Pegasus, trains clients in its use, and assists those clients throughout every stage of the deployment and operation of the spyware." [Dkt. No. 1] at

[11] As previously discussed, the conduct described in the Complaint was allegedly committed by Saudi Arabia and the UAE, [Dkt. No. 1] at ¶ 108 ("Saudi Arabia . . . leveraged its relationship with a key ally, the United Arab Emirates, to install Pegasus on her phones."); the "text message" with a "disabled Pegasus link" was sent by "an agency of the UAE," id. at ¶ 102; Pegasus was "manually installed" in the UAE by "Emirati intelligence officers," id. at ¶¶ 106 & n.54; plaintiff's private communications were "relayed to the Saudis, via the UAE," id. at ¶ 113, and "invaded by agents of an authoritarian government," id. at ¶ 129. None of these allegations establish a sufficient connection between NSO Group and Virginia, or provide a sufficient plausible basis for the Court to conclude that plaintiff was in Virginia at this time.

¶¶ 46-48, 66-71, 77. But plaintiff fails to link that allegation to the conduct of the Saudi and Emirati officials who were NSO Group's customers and the end users of the Pegasus technology that surveilled her.

Defendants also contend that plaintiff has failed to allege she actually lived in Virginia when her devices were accessed. According to defendants, "[plaintiff] did not move to the [United States] until she decided to seek asylum after Jamal Khashoggi was killed in October 2018." [Dkt. No. 46] at 2 (quoting Supp. Akro. Decl. Ex. A). They argue that plaintiff "lived in Dubai in April 2018; traveled to Washington, D.C. in June 2018 to marry Mr. Khashoggi in a religious ceremony but 'did not have residence in the [United States] at that time'; and only moved to the United States after Mr. Khashoggi was killed." See [Dkt. No. 46] at 3.

During oral argument, plaintiff's counsel proffered new arguments and facts that were not contained in the Complaint. For example, counsel claimed that plaintiff began living in Virginia some time before her engagement to Jamal in April 2018, and regularly visited the Commonwealth before that time. Moreover, counsel asserted that plaintiff and Jamal were married in June 2018, after which time they moved into a home together in Virginia. Despite these newly postulated facts, counsel did not clarify plaintiff's location when the alleged Pegasus links were sent to her phones or precisely where she was located between the alleged installation of Pegasus on her phones in the Dubai airport in April 2018 and her moving in with her husband later that summer.

Additionally, plaintiff fails to rebut defendants' persuasive argument that at best she has pleaded that NSO Group's Pegasus technology infiltrated her devices in Virginia only because of intervening acts by third-party sovereigns. See St. Jarre v. Heidelberger Druckmaschinen, A.G., 19 F.3d 1430 (4th Cir. 1994) ("The exercise of personal jurisdiction over a foreign manufacturer,

whose product reached the forum state because of intervening sales by third parties, would be unfair and unreasonable."). On this record, plaintiff has not adequately alleged that her claims arose out of conduct defendants directed at and conducted in Virginia.

c. Constitutional due process

Due process requires that a court's exercise of specific jurisdiction "be constitutionally reasonable." Consulting Eng'rs Corp, 561 F.3d at 278. Under that requirement, courts "consider additional factors to ensure the appropriateness of the forum," including "(1) the burden on the defendant of litigating in the forum; (2) the interest of the forum state in adjudicating the dispute; (3) the plaintiff's interest in obtaining convenient and effective relief; (4) the shared interest of the states in obtaining efficient resolution of disputes; and (5) the interests of the states in furthering substantive social policies." Id. at 279; see also Burger King, 471 U.S. at 477. At this step of the specific personal jurisdiction analysis, the burden shifts to defendants to present a compelling case that jurisdiction would be unreasonable. Burger King, 471 U.S. at 477. The more attenuated the contacts with the forum state, the less a defendant must show in terms of unreasonableness to defeat the court's exercise of jurisdiction.

Plaintiff argues that Virginia has a strong interest in resolving this dispute, "as declining to assert jurisdiction would grant hackers who have invaded the privacy of Virginia residents 'carte balance to [surveil] with impunity.'" [Dkt. No. 1] at 5 (quoting Verizon Online Servs., 203 F. Supp. 2d at 612). Plaintiff further contends that, as a Virginia resident, she has a substantial interest in vindicating her rights in this Court and would be burdened if forced to litigate her claims in Israel.

The factors counseling against personal jurisdiction being constitutionally reasonable are substantial. First, NSO Group is incorporated in Israel, owns no property in Virginia, and has no

employees or persons authorized to act on its behalf in Virginia.[12] Additionally, NSO Group is without evidence or witnesses in Virginia, most of which are located in Israel, Saudi Arabia, and the UAE.[13] The foreign relations implications involved in this civil action would likely impose substantial restrictions on parties' discovery and impair their abilities to access relevant documents to present or defend a position. Plaintiff is correct that litigating this civil action in Virginia would be more convenient for her, but that alone does not automatically outweigh the burden on defendants if they were forced to litigate in this district. See Grizzard v. LG Chem Ltd., 641 F. Supp. 3d 282, 292 (E.D. Va. 2022) (finding jurisdiction unreasonable even though "a number of . . . factors may point in [p]laintiff's favor" because "'[d]ue process limits on the State's adjudicative authority principally protect the liberty of the nonresident defendant—not the convenience of the plaintiffs or third parties'" (quoting Walden, 571 U.S. at 284)).

Moreover, NSO Group argues that this action "poses severe threats to Israel's sovereignty because Israel regulates and reviews [NSO Group's] operations—including the licensing decisions that plaintiff seeks to challenge under Virginia law—and details of Israel's decisions would have to be disclosed for [NSO Group] to defend this action." [Dkt. No. 13] at 13; Ex. 1 at ¶¶ 6-11, 16. Israel likewise has "a strong national-security interest in the subject-matter of this action, and [the Israeli government] prohibits NSO [Group] from disclosing in this action broad swaths of information relevant to refuting plaintiff's claims." [Dkt. No. 13] at 13. The United States Supreme Court has also cautioned against extending state long arm statutes in

[12] The Complaint has not alleged that Westbridge was involved in surveilling plaintiff.

[13] Defendants argue that requiring this civil action to be litigated in the United States would also unduly interfere with the sovereignty of the foreign nations which may be required to participate. "Where, as here, the defendant is from a foreign nation rather than another state, the sovereignty barrier is high and undermines the reasonableness of personal jurisdiction." Amoco Egypt Oil Co. v. Leonis Nav. Co., 1 F.3d 848, 852 (9th Cir. 1993).

an international context. See Asahi Metal Indus. Co. v. Superior Ct. of Cal., Solano Cnty., 480 U.S. 102, 115 (1987). Here, while defendants have presented no evidence as to a particular interest, the state of Israel has some presumable interest in adjudicating conflicts concerning its corporate citizens. See Harris Rutsky & Co. Ins. Servs. v. Bell & Clements Ltd., 328 F.3d 1122, 1133 (9th Cir. 2003) ("While [defendant] has presented no evidence of the United Kingdom's particular interest in adjudicating this suit, we may presume for present purposes that there is such an interest."). On balance—factoring in plaintiff's inability to plausibly demonstrate that NSO Group directed its alleged conduct at her in Virginia—the Court finds that exercising specific personal jurisdiction over defendants in this district would offend constitutional due process.

d. Fed. R. Civ. P. 4(k)(2)

Plaintiff's alternative argument for personal jurisdiction under Fed. R. Civ. P. 4(k)(2) fares no better. Under Rule 4(k)(2), personal jurisdiction can be found where 1) the case arises under federal law, 2) the defendant is not subject to personal jurisdiction in any other state, and 3) the defendant's "contacts with the United States as a whole" are sufficient to satisfy due process requirements. Base Metal Trading, Ltd. v. OJSC Novokuznetsky Aluminum Factory, 283 F.3d 208, 215 (4th Cir. 2002). Plaintiff's argument for personal jurisdiction under Rule 4(k)(2) fails to meet all three of Base Metal's requirements.[14]

To satisfy the second requirement for Rule 4(k)(2) jurisdiction, plaintiff must demonstrate that NSO Group is not subject to personal jurisdiction in any state; however,

[14] Although the Court declines to address defendants' Motion to Dismiss with respect to Fed. R. Civ. P. 12(b)(6), defendants have made a strong argument that plaintiff's only federal claim is time barred. If this were so, it would provide an additional basis for concluding that personal jurisdiction over the defendants is not available under Rule 4(k)(2).

plaintiff has actually cited to the case WhatsApp, Inc. v. NSO Group Technologies Limited, 472 F. Supp. 3d 649 (N.D. Cal. 2020), in which the district court found that NSO Group is subject to specific personal jurisdiction in California based on its direct targeting of WhatsApp's servers in that forum. That finding was not disturbed on appeal. WhatsApp, Inc. v. NSO Grp. Techs. Ltd., 17 F.4th 930 (9th Cir. 2021). The California civil action alone destroys plaintiff's reliance on Rule 4(k)(2) for personal jurisdiction. In addition, plaintiff's primary argument in this civil action is that NSO Group is subject to personal jurisdiction in Virginia, which directly contradicts her reliance on Rule 4(k)(2). In Base Metal, the Fourth Circuit refused to allow a plaintiff to "present inconsistent alternative positions in a case" when invoking Rule 4(k)(2). Id.

As to the final requirement, the same constitutional due process analysis conducted with respect to specific personal jurisdiction counsels against plaintiff's argument under Rule 4(k)(2). The notions of "fair play and substantial justice" do not favor suit in Virginia. For all these reasons, plaintiff has failed to satisfy the requirements of Rule 4(k)(2). Therefore, she has failed to establish that the Court has personal jurisdiction over defendants. [15]

[15] In her briefing and at oral argument, plaintiff did not request leave to amend should the Court grant defendants' Motion to Dismiss. Accordingly, the Complaint will be dismissed with prejudice.

III. CONCLUSION

The Court has a responsibility to decide preliminary issues, such as jurisdiction, before reaching the merits of a claim. Although plaintiff presents a compelling description of her loss from the alleged conduct of defendants, the Court must nevertheless evaluate the issue of jurisdiction under established legal principles, which lead the Court to conclude that it does not have personal jurisdiction over defendants. For these reasons, defendants' Motion to Dismiss will be granted by an Order to be issued with this Memorandum Opinion.

Entered this 26th day of October, 2023.

Alexandria, Virginia

/s/
Leonie M. Brinkema
United States District Judge