Nika Aldrich, OSB No. 160306
naldrich@schwabe.com
SCHWABE, WILLIAMSON & WYATT, P.C.
1211 SW 5th Ave., Suite 1900
Portland, OR 97204
Telephone: 503-222-9981
Facsimile: 503-796-2900

Anthony T. Pierce (*pro hac vice*)
apierce@akingump.com
Caroline L. Wolverton (*pro hac vice)*
cwolverton@akingump.com
AKIN GUMP STRAUSS HAUER & FELD LLP
2001 K St., N.W.
Washington, D.C. 20006
Telephone: (202) 887-4000
Facsimile: (202) 887-4288

Natasha G. Kohne (*pro hac vice*)
nkohne@akingump.com
AKIN GUMP STRAUSS HAUER & FELD LLP
580 California St.
Suite 1500
San Francisco, CA 94104
Telephone: (415) 765-9500
Facsimile: (415) 765-9501

Attorneys for Defendant DarkMatter Group

Clifford S. Davidson, OSB No. 125378
csdavidson@swlaw.com
SNELL & WILMER L.L.P.
1455 SW Broadway, Suite 1750
Portland, OR 97201
Telephone: 503-624-6800
Facsimile: 503-624-6888

Attorney for Defendants Marc Baier, Ryan Adams, and Daniel Gericke

IN THE UNITED STATES DISTRICT COURT

DISTRICT OF OREGON

LOUJAIN HATHLOUL ALHATHLOUL, Plaintiff, v. DARKMATTER GROUP, MARC BAIER, RYAN ADAMS, and DANIEL GERICKE, Defendants.	Case No. 3:21-cv-01787-IM **DEFENDANTS' MOTION TO DISMISS AND MEMORANDUM OF LAW IN SUPPORT** **REQUEST FOR ORAL ARGUMENT**

DEFENDANTS' MOTION TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES:

STATUTES:

OTHER AUTHORITIES:

LOCAL RULE 7-1 CERTIFICATION

The undersigned counsel hereby certifies that on May 19, 2022, counsel discussed the substance of this Motion with counsel for Plaintiffs. The parties were unable to resolve the dispute.

MOTION

Defendants DarkMatter Group ("DarkMatter"), Marc Baier, Ryan Adams, and Daniel Gericke hereby move this Court to dismiss this case pursuant to Fed. R. Civ. P. 12(b).

INTRODUCTION

Plaintiff Loujain Hathloul Alhathloul, a Saudi activist who resides abroad, brings this suit against Defendants DarkMatter (a United Arab Emirates company with no U.S. presence) and three former DarkMatter employees (who all reside abroad). Plaintiff alleges that DarkMatter hacked her phone when she was located in the UAE, causing her harm in the UAE and Saudi Arabia. Despite the wholly foreign nature of her claims and the foreign residence of all parties, Plaintiff brings suit in the United States. This case should not proceed beyond the pleadings stage, as her claims are fatally deficient in multiple respects.

First, Plaintiff's transparent attempt to manufacture personal jurisdiction in the United States should be rejected. Her complaint alleges no jurisdictionally significant connection between Defendants, this litigation, and the United States. She thus fails to show that this Court has jurisdiction over DarkMatter or its former employees (including Defendant Ryan Adams, whom Plaintiff incorrectly states is domiciled in Oregon). Indeed, the *only* U.S. connection Plaintiff alleges is the happenstance that certain text messages allegedly sent by DarkMatter from a location abroad passed through U.S. servers, which allegedly later caused her to suffer harm in foreign countries. But under well-established law, such allegations are insufficient to establish personal jurisdiction in the United States. Otherwise, the United States would become the universal forum for a potentially limitless number of claims involving electronic communications between wholly

foreign parties. That explains why the Ninth Circuit "has never decided that personal jurisdiction is proper over a private foreign entity solely because that entity engaged in tortious conduct from a location outside of the United States by remotely accessing servers located in the United States." *Hungerstation LLC v. Fast Choice LLC*, 857 F. App'x 349, 351 (9th Cir. 2021). This case should not be the first.

Second, Plaintiff fails to state any plausible claim for relief. Plaintiff's first claim, for violation of the Computer Fraud and Abuse Act (CFAA), should be dismissed because her "information and belief" allegations fail to connect any of the Defendants to the alleged hacking of Plaintiff's phone, and cannot satisfy the statutory "loss" standard in any event. Plaintiff's second claim, for conspiracy to violate the CFAA, is also barred—not only because the underlying claim is deficient, but also because of the fundamental principle that a corporation cannot conspire with its own employees as a matter of law.

Third, the Court lacks jurisdiction over Plaintiff's third claim, under the Alien Tort Statute, both because it is impermissibly extraterritorial and because it seeks an unprecedented expansion of liability that would force this Court to adjudicate the legality of the actions of foreign sovereigns taken in their own territories.

Finally, if Plaintiff's agency allegations are accepted as true—as they must be—Defendants are entitled to common law conduct-based immunity

The Court should thus dismiss Plaintiff's claims with prejudice.

BACKGROUND

Plaintiff alleges that in late 2015 or early 2016, the UAE government retained Defendant DarkMatter, a UAE company, to provide cybersecurity services. (*See* Complaint (ECF 1) ¶¶ 6, 67.) Around the same time, Defendants Marc Baier, Ryan Adams, and Daniel Gericke, who had

previously worked for a U.S. company that provided similar services for the UAE government, joined DarkMatter as employees. (*See id.* ¶ 69.)

According to Plaintiff's "information and belief" allegations, at some point before March 2018, DarkMatter allegedly hacked (from the UAE) her iPhone (located in the UAE) by sending an "iMessage" to Plaintiff's "Messages" application. (*See* ECF 1 ¶¶ 87-104; *see, e.g.*, *id.* ¶ 104 ("On information and belief, DarkMatter . . . deploy[ed] an iOS exploit and malware to Ms. Alhathloul's device[.]"); *id.* ¶ 112 ("On information and belief, this malware . . . allowed DarkMatter to receive real-time location information to monitor the movements and whereabouts of Ms. Alhathloul."); *id.* ¶¶ 103, 108, 109, 110 ("information and belief")). She does not allege that Defendants directed their conduct to the United States specifically.

Plaintiff alleges that the hack eventually led to her arrest in the UAE, rendition to Saudi Arabia, and detention and torture there. (*Id.* ¶¶ 117-118, 122-124.) She asserts claims against all Defendants for violating and conspiring to violate the CFAA (counts one and two), and a claim solely against Baier, Adams, and Gericke under the ATS (count three). (*Id.* pp. 32-38.)

ARGUMENT

I. THE COURT LACKS PERSONAL JURISDICTION OVER ALL DEFENDANTS

A. Legal Standard

"In opposing a defendant's motion to dismiss for lack of personal jurisdiction" under Rule 12(b)(2) of the Federal Rules of Civil Procedure, "the plaintiff bears the burden of establishing that jurisdiction is proper." *Mavrix Photo, Inc. v. Brand Technologies, Inc.*, 647 F.3d 1218, 1223 (9th Cir. 2011). The court must resolve "conflicts between the parties" in the plaintiff's favor when the plaintiff provides some evidence to support her position, *Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 800 (9th Cir. 2004), but "disputed allegations in the complaint that are not

supported with evidence or affidavits cannot establish jurisdiction," *AMA Multimedia, LLC v. Wanat*, 970 F.3d 1201, 1207 (9th Cir. 2020).

Under Rule 4(k)(2), "[f]or a claim that arises under federal law," a court may exercise personal jurisdiction over a defendant "not subject to jurisdiction in any state's courts of general jurisdiction" if "exercising jurisdiction is consistent with the United States Constitution and laws." FED. R. CIV. P. 4(k)(2). Thus, Rule 4(k)(2) requires (1) a federal claim, (2) a defendant not subject to personal jurisdiction in any state, and (3) that "the federal court's exercise of personal jurisdiction . . . comport[s] with due process." *Holland Am. Line Inc. v. Wartsila N. Am., Inc.*, 485 F.3d 450, 461 (9th Cir. 2007). Because the first two requirements are undisputed with respect to all Defendants except Adams (*see infra* pp. 13-14), only due process is at issue here.

Consistent with due process, courts can exercise "two kinds of personal jurisdiction: general (sometimes called all-purpose) jurisdiction and specific (sometimes called case-linked) jurisdiction." *Ford Motor Co. v. Montana Eighth Jud. Dist. Ct.*, 141 S. Ct. 1017, 1024 (2021). For specific jurisdiction—the only form of jurisdiction Plaintiff alleges with respect to all Defendants besides Adams—"[d]ue process requires that a defendant who is not present in the forum has 'certain minimum contacts' with the forum 'such that the maintenance of the suit does not offend traditional notions of fair play and substantial justice.'" *AMA*, 970 F.3d at 1208 (quoting *International Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945)). The inquiry under Rule 4(k)(2) is "nearly identical to the traditional personal jurisdiction analysis with one significant difference: rather than considering contacts between [the defendant] and the forum state, [courts] consider contacts with the nation as a whole." *AMA*, 970 F.3d at 1208 (quoting *Holland Am. Line*, 485 F.3d at 462); *see also Glencore Grain Rotterdam B.V. v. Shivnath Rai Harnarain Co.*, 284 F.3d 1114, 1126 (9th Cir. 2002) ("[T]he rule provides for what amounts to a federal long-arm statute in a

narrow band of cases in which the United States serves as the relevant forum for a minimum contacts analysis.").

The minimum contacts test requires a plaintiff to satisfy each of three elements:

> (1) The non-resident defendant must purposefully direct his activities or consummate some transaction with the forum or [a] resident thereof; or perform some act by which he purposefully avails himself of the privilege of conducting activities in the forum, thereby invoking the benefits and protections of its laws;
>
> (2) the claim must be one which arises out of or relates to the defendant's forum-related activities; and
>
> (3) the exercise of jurisdiction must comport with fair play and substantial justice, i.e., it must be reasonable.

Freestream Aircraft (Bermuda) Ltd. v. Aero Law Grp., 905 F.3d 597, 603 (9th Cir. 2018).

B. The Court Lacks Personal Jurisdiction Over DarkMatter

Without asserting any particular theory of personal jurisdiction, Plaintiff alleges that exercising jurisdiction over DarkMatter would be "consistent with the Constitution and United States law." (ECF 1 ¶ 11.) On the contrary, Plaintiff's allegations against DarkMatter fail to satisfy each prong of the "minimum contacts" test.

1. DarkMatter Did Not Purposefully Direct Any Activities At The United States

Under the first prong, when a plaintiff's claims "sound in tort," the relevant question is whether the non-resident defendant "purposefully directed activities at the United States." *AMA*, 970 F.3d at 1208; *see also Burton v. Air France – KLM*, No. 3:20-cv-1085-IM, 2020 WL 7212566, at *3 (D. Or. Dec. 7, 2020) (purposeful direction analysis applies to intentional torts). When the "allegedly tortious conduct takes place *outside* the forum" and allegedly "has effects inside the forum," the Ninth Circuit determines purposeful direction based on an "effects test[.]" *AMA*, 970 F.3d at 1208 (citing *Calder v. Jones*, 465 U.S. 783 (1984)). "Under this test, the defendant allegedly must have (1) committed an intentional act, (2) expressly aimed at the forum . . . , [and]

(3) causing harm that the defendant knows is likely to be suffered in the forum[.]" *Id.* at 1209 (internal quotation marks omitted). "[R]andom, fortuitous, or attenuated contacts" with the United States, or unilateral "contacts between the plaintiff (or third parties) and the forum," cannot support jurisdiction. *Walden v. Fiore*, 571 U.S. 277, 284, 286 (2014); *see id.* at 284 ("[T]he relationship must arise out of contacts that the defendant *himself* creates with the forum," not conduct by third parties) (internal quotation marks omitted).

As explained below, although Plaintiff alleges "intentional acts," she cannot show that DarkMatter "expressly aimed" them at the forum, or that they "caus[ed] harm" in the forum.

a. DarkMatter's Alleged Conduct Was Not "Expressly Aimed" At The United States

Plaintiff has not plausibly alleged that DarkMatter "aim[ed]" any "intentional conduct" at the United States. *See AMA*, 970 F.3d at 1209 n.5. There is no dispute that DarkMatter does not do business in the United States, operate offices in the United States, or have employees in the United States. Instead, Plaintiff attempts to manufacture jurisdiction based on DarkMatter's alleged use of Apple servers located in the United States to gain access to the data in her iPhone.

But the Ninth Circuit "has never decided that personal jurisdiction is proper over a private foreign entity solely because that entity engaged in tortious conduct from a location outside of the United States by remotely accessing servers located in the United States." *Hungerstation*, 857 F. App'x at 351 (rejecting such a theory). As in *Hungerstation*, the sole alleged connection between DarkMatter and the United States shows that "the location of the servers was fortuitous." *Id.* Such fortuitous contacts with a U.S. server alone, however, have never given rise to U.S.-based jurisdiction. *See id.*; *see also Broidy Cap. Mgmt., LLC v. Qatar*, No. CV 18-2421-JFW(Ex), 2018 WL 9943551, at *7 (C.D. Cal. Aug. 22, 2018) ("[T]he location of the servers appears to be 'random,' 'fortuitous,' or 'attenuated' to Defendants' purported actions and intent to hack

Plaintiffs' computer systems and accounts to obtain confidential and private information[.]"); *Future World Elecs., LLC v. Results HQ, LLC*, No. CV 17-17982, 2018 WL 2416682, at *3 (E.D. La. May 29, 2018) ("Here, the location of the server in Louisiana was fortuitous. There is no indication that either plaintiff or defendants had any control over the server's location, or that the location had any bearing on defendants' conduct."); *Rosen v. Terapeak, Inc.*, No. CV-15-00112-MWF (Ex), 2015 WL 12724071, at *9 (C.D. Cal. Apr. 28, 2015) (rejecting personal jurisdiction based on the "use of eBay servers in California to obtain . . . photographs").[1] Had Apple's servers been located in Canada, Ireland, or the UAE, Plaintiff's allegations regarding the parties' intentional conduct would be the same. Because "none of [the] challenged conduct had anything to do with [the United States] itself," the location of the servers is not "a proper basis for jurisdiction." *Walden*, 571 U.S. at 289, 290.

Even if intentionally targeting servers that happened to be located in the United States could constitute "express aiming" in some circumstances, Plaintiff's allegations would still not be enough. The gravamen of Plaintiff's Complaint is not that DarkMatter intentionally targeted *Apple's U.S. servers*; it is that DarkMatter targeted *her.* And her allegations of supposed "targeting" of Apple's servers are hyper-technical descriptions of Apple's processes that are triggered by *anyone* who sends iMessages to an iPhone located anywhere in the world. Indeed, those descriptions appear to have been cribbed from Apple's website generally describing how iMessaging works. *Compare* ECF 1 ¶¶ 89, 90 (alleging DarkMatter "retriev[ed]" Plaintiff's "encryption and routing information from Apple's identity servers," "encrypt[ed] the iMessage,"

[1] *See also Man-D-Tec, Inc. v. Nylube Prods. Co.*, No. CV-11-1573-PHX-GMS, 2012 WL 1831521, at *2 (D. Ariz. May 18, 2012); *Browne v. McCain*, 612 F. Supp. 2d 1118, 1124 (C.D. Cal. 2009); *Chang v. Virgin Mobile USA, LLC*, No. 3:07-CV-1767-D, 2009 WL 111570, at *3 (N.D. Tex. Jan. 16, 2009); *Doe v. Geller*, 533 F. Supp. 2d 996, 1009 (N.D. Cal. 2008); *Ray v. Experian*, No. 3:07-cv-1114-R, 2008 WL 4245459, at *3 (N.D. Tex. Nov. 30, 2007).

and "sen[t] the iMessage to the Apple Push Notification Service"), *with* Apple Platform Security, *iMessage security overview* at 178 (May 2022), https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf (when a user sends an iMessage to a phone number or email address, "the device contacts the Apple Identity Service" to "retrieve" the encryption and routing information of the "addressee"), and Apple Platform Security, *how iMessage sends and receives messages securely* (Feb. 18, 2021), https://support.apple.com/guide/security/how-imessage-sends-and-receives-messages-sec70e68c949/1/web/1 (outgoing iMessages are "individually encrypted" before being "dispatched to the APNs [Apple Push Notification Service] for delivery").

Plaintiff's allegations thus boil down to the idea that by hitting "send," an iMessage user triggers Apple's automated encryption, routing, and delivery process through servers that happen to be based in the United States, and thereby subjects the sender to personal jurisdiction in the United States. (*See* ECF 1 ¶¶ 89-104.) Without more, any nexus to the United States necessarily results from Apple's "fortuitous" connection to the United States—*i.e.*, a "third party['s]" decision to host servers here, rather than abroad—and not the sender's "intentional conduct." *Walden*, 571 U.S. at 286. Otherwise, federal courts would presumptively have personal jurisdiction over any foreign party with no connection to the United States other than that their claims involve iMessages that Apple has unilaterally chosen to route through U.S. servers. Given that the United States hosts servers from many of the largest communications technology companies in the world—Google, Twitter, and Microsoft, to name a few—Plaintiff's theory would result in essentially universal jurisdiction over a truly breathtaking scope of claims involving communications between wholly foreign parties. *Cf. Man-D-Tec*, 2012 WL 1831521, at *2 ("If the mere location of a server could create personal jurisdiction, any state where a server is located would have personal jurisdiction over any user of that server."). This Court should reject that untenable result. Because

DarkMatter's alleged conduct was not "expressly aimed at" the United States, the Court should dismiss the Complaint. *See AMA*, 970 F.3d at 1209 (applying *Calder*, 465 U.S. 783).

b. DarkMatter's Alleged Conduct Did Not Cause Harm That DarkMatter Knew Would Likely Be Suffered In The United States

Plaintiff's allegations also fail to establish purposeful direction under the Ninth Circuit's "effects test" because they do not establish that DarkMatter "caus[ed] harm that the defendant knows is likely to be suffered in the forum[.]" *AMA*, 970 F.3d at 1209. Plaintiff must allege that the United States was "the forum in which the defendant's actions were felt, whether or not the actions themselves occurred within the forum." *Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme*, 433 F.3d 1199, 1205-1206 (9th Cir. 2006) (en banc). In other words, the "defendant's actions" must have been "performed for the very purpose of having their consequences felt in the forum state." *Brown v. Service Grp. of Am., Inc.*, No. 3:20-cv-2205-IM, 2022 WL 43880, at *3 (D. Or. Jan. 5, 2022) (quoting *Brainerd v. Governors of the Univ. of Alberta*, 873 F.2d 1257, 1260 (9th Cir. 1989)); *see also Walden*, 571 U.S. at 290 (even "injury to a forum resident" is insufficient unless "defendant's conduct connects him to the forum in a meaningful way"). Thus, at a minimum, "some significant amount of harm" must have been "suffered" in the forum for the Complaint to survive a motion to dismiss. *Dole Food Co. v. Watts*, 303 F.3d 1104, 1112-1113 (9th Cir. 2002); *see also AMA*, 970 F.3d at 1212 (dismissing case where "the United States was not 'the focal point . . . of the harm suffered'") (quoting *Walden*, 517 U.S. at 287).

Plaintiff's allegations do not come close to showing that DarkMatter caused significant and foreseeable harm in the United States. Plaintiff alleges that she was harmed only in the UAE and Saudi Arabia and does not allege *any* harm suffered in the United States, let alone harm that DarkMatter knew was "likely to be suffered" there. *AMA*, 970 F.3d at 1209. On the contrary, Plaintiff's allegations negate the possibility that the "very purpose" of DarkMatter's actions was

to cause harm that would be "felt" in the United States, *Brown*, 2022 WL 43880, at *3, given that Plaintiff repeatedly alleges that DarkMatter's purpose was to provide information to foreign governments, ultimately leading to harm abroad. (ECF 1 ¶¶ 112-130.) The lack of U.S. harm thus provides an independent basis for dismissal. *See Brown*, 2022 WL 43880, at *3 (dismissing complaint for failure to establish defendant knew harm would likely be suffered in Oregon); *Broidy*, 2018 WL 9943551, at *7-8 (dismissing complaint alleging hacking of servers located in the forum in part because "it was not foreseeable that the . . . Defendants' conduct in other forums was likely to cause harm in" the forum); *Traeger Pellet Grills, LLC v. Deadwood Biofuels, LLC*, No. 3:11-cv-01221-JE, 2012 WL 4040211, at *5 (D. Or. June 21, 2012) (even though defendant's "efforts may have been intentionally directed toward Oregon," dismissal was appropriate because defendant's actions did not "cause[] harm that [defendant] knew would likely be suffered in [Oregon]").

2. Plaintiff's Claims Do Not Arise Out Of Or Relate To DarkMatter's U.S. Contacts

Plaintiff's allegations against DarkMatter also fail the second prong of the minimum contacts test, which requires that the plaintiff's claims "arise out of or relate to the defendant's contacts with the forum." *Ford*, 141 S. Ct. at 1025 (internal quotation marks omitted). That means "there must be an affiliation between the forum and the underlying controversy, principally, an activity or an occurrence that takes place in the forum . . . and is therefore subject to [its] regulation." *Id.* (internal quotation marks and alteration omitted). This connection between the plaintiff's claims and the United States must be substantial enough that, based on the defendant's litigation-related conduct, the defendant can "reasonably anticipate" its "exposure" to suit in the United States—such as when the defendant "enjoys the benefits and protection of [the forum's] laws." *Id.* at 1027, 1029.

For the reasons noted above, Plaintiff's claims do not "arise out of or relate to" any intentional contacts between DarkMatter and the United States. *Ford*, 141 S. Ct. at 1025. Plaintiff has not alleged the existence of any litigation-related contacts with the United States.[2] And DarkMatter certainly did not enjoy the benefit or protection of United States law, or otherwise do anything that could lead it to "reasonably anticipate" being haled into U.S. court, merely by allegedly sending a text message from a location abroad to a phone located abroad. *See id.* at 1027.

3. Exercising Jurisdiction Over DarkMatter Would Be Unreasonable

Finally, Plaintiff's allegations fail the third prong of the minimum contacts test because exercising jurisdiction over DarkMatter would be unreasonable. "To evaluate reasonableness," the Ninth Circuit applies "a seven-factor balancing test," weighing:

> (1) the extent of the defendant's purposeful interjection into the forum state's affairs; (2) the burden on the defendant of defending in the forum; (3) the extent of conflict with the sovereignty of the defendant's [home forum]; (4) the forum state's interest in adjudicating the dispute; (5) the most efficient judicial resolution of the controversy; (6) the importance of the forum to the plaintiff's interest in convenient and effective relief; and (7) the existence of an alternative forum.

Freestream, 905 F.3d at 607. The Supreme Court has warned that "[g]reat care and reserve should be exercised when extending our notions of personal jurisdiction into the international field." *Asahi Metal Indus. Co. v. Superior Ct. of Cal., Solano Cnty.*, 480 U.S. 102, 115 (1987). Thus, courts should not "find the serious burdens on an alien defendant outweighed by minimal interests on the part of the plaintiff or the forum." *Id*. But that is precisely what Plaintiff asks this Court to do. Indeed, all seven factors weigh against exercising personal jurisdiction over DarkMatter:

[2] Many of Plaintiff's allegations have no connection to her causes of action. For example, Plaintiff alleges that the UAE previously contracted with a U.S. company to develop and use hacking technology, and that DarkMatter has used the same technology and employees as that U.S. company. (*See* ECF 1 ¶¶ 52-67.) But only DarkMatter's contacts related to Plaintiff's claims can support personal jurisdiction—the general history of DarkMatter, its technology, and its employees is irrelevant. At a minimum, such historical contacts cannot establish "express aiming" for the alleged tort at issue here. *AMA*, 970 F.3d at 1209 n.5.

1. texting a foreign person's iPhone from a location abroad to a location abroad presents no "purposeful interjection" in the United States' affairs, *see Hungerstation*, 857 F. App'x at 352 (purposeful interjection "negligible" when alleged misconduct "aimed at a nonresident") (quoting *Paccar Int'l, Inc. v. Commercial Bank of Kuwait, S.A.K.*, 757 F.2d 1058, 1065 (9th Cir. 1985));

2. DarkMatter, a UAE company with no U.S. connections, would be significantly burdened defending a lawsuit in this distant forum, *see Asahi*, 480 U.S. at 114 ("The unique burdens placed upon one who must defend oneself in a foreign legal system should have significant weight in assessing the reasonableness of stretching the long arm of personal jurisdiction over national borders.");

3. there is an obvious conflict with the sovereignty of DarkMatter's home forum because Plaintiff's allegations concern events that occurred largely in the UAE and directly implicate the UAE government, *see, e.g.*, *Paccar*, 757 F.2d at 1065 (conflict with sovereignty due to foreign government's interest in the dispute, even without the sort of "foreign policy overtones" present here);

4. the United States has no apparent interest in adjudicating this dispute between foreign companies and foreign residents regarding foreign conduct, *see, e.g.*, *Asahi*, 480 U.S. at 114 (forum's interest at least "considerably diminished" in a dispute between foreign parties), let alone in encouraging the filing of a potentially limitless number of claims involving foreign electronic communications that merely pass through U.S. servers;

5. resolving the controversy here would be inefficient because all relevant parties, documents, and witnesses are located abroad, *see, e.g., Hungerstation*, 857 F. App'x at 352;

6. for the same reason, Plaintiff's interest in convenient and effective relief in this forum is diminished, *see id.*; and

7. Plaintiff has not shown or even alleged that alternative forums are unavailable, *see id.*

In light of these factors, there is a "compelling case that the exercise of jurisdiction would not be reasonable." *Schwarzenegger*, 374 F.3d at 802 (internal quotation marks omitted).

For each of the above reasons, the Court does not have personal jurisdiction over DarkMatter.

C. The Court Lacks Personal Jurisdiction Over Individual Defendants Marc Baier and Daniel Gericke

Plaintiff also states that Baier and Gericke are subject to this Court's personal jurisdiction under Rule 4(k)(2). But the complaint merely assumes that the Court has specific personal jurisdiction over Baier and Gericke based on the same allegations regarding DarkMatter's use of Apple servers to access Plaintiff's iPhone. As discussed, those allegations are not enough.

Even if otherwise, the allegations as to Baier and Gericke are weaker than those related to DarkMatter. Plaintiff does not allege that Baier or Gericke accessed her iPhone or had any role in the alleged scheme. She alleges that Baier and Gericke merely participated in the general development of DarkMatter's alleged hacking capabilities and had inauthentic Apple accounts. And while the Complaint alleges that Baier and Gericke entered into deferred prosecution agreements based on their employment with DarkMatter, it does not allege that the agreements had anything to do with actions taken against Plaintiff (and in fact, those agreements do not refer to Alhathloul explicitly or implicitly).[3]

D. The Court Lacks Personal Jurisdiction Over Individual Defendant Ryan Adams

Plaintiff alleges that Adams is subject to the Court's personal jurisdiction because "[o]n information and belief," he is "domiciled" in Oregon. (ECF 1 ¶¶ 9, 12.) But in fact, Adams is *not* domiciled in Oregon. (*See* Adams Decl. ¶ 2.) Although his wife's family lives there, Adams has never resided in Oregon. (*Id.* ¶¶ 3, 7.) He does not own (and has never owned) real property in Oregon, does not have (and has never had) an Oregon driver's license, and is not (and has never

[3] The Complaint's allegation that Baier is a United States citizen (ECF 1 ¶ 7), does not give rise to personal jurisdiction. *See Pebble Beach Co. v. Caddy*, 453 F.3d 1151, 1153, 1160 (9th Cir. 2006) (no personal jurisdiction under Rule 4(k)(2) even though the defendant, located in England, was a U.S. citizen). And because Baier and Gericke are domiciled in the UAE and Singapore, respectively, substantially the same "reasonableness" analysis that applies to DarkMatter applies to them.

been) an Oregon voter. (*Id.* ¶¶ 4, 5, 6.) Nor does the Complaint contain any other allegations connecting Adams to Oregon.

Thus, Plaintiff has failed to establish that jurisdiction over Adams is proper under the Oregon long-arm statute. *See* OR. R. CIV. P. 4. Plaintiff alleges no other basis for exercising jurisdiction over Adams. Regardless, Rule 4(k)(2) does not provide jurisdiction over Adams for the same reasons that it does not provide jurisdiction over Baier and Gericke.

II. PLAINTIFF FAILS TO STATE A CLAIM FOR WHICH RELIEF MAY BE GRANTED

Under Rule 12(b)(6), a complaint must plead facts that, if accepted as true, would "state a claim for relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). A claim is plausible "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.*

A. Plaintiff's CFAA Claim (Count One) Should Be Dismissed

The CFAA, a criminal statute prohibiting unauthorized computer access, provides a civil cause of action for "[a]ny person who suffers damage or loss by reason of a violation" of the statute in certain circumstances. 18 U.S.C. § 1030(g). Plaintiff fails to state a claim under the CFAA for two reasons: she fails to plausibly link any Defendant to the unauthorized computer access, and her allegations fail to satisfy the statutory "loss" standard.

1. The Complaint Contains No Well-Pleaded Facts Supporting The CFAA Claim

The Complaint spends over one hundred paragraphs describing Plaintiff's background, alleged actions by non-defendants UAE and Saudi Arabia, the individual Defendants' alleged work for another company, the individuals Defendants' alleged work for DarkMatter, alleged hackings of individuals not party to this action, and DarkMatter's alleged hacking technology and methodology. But notably absent is a non-speculative, non-conclusory connection between

Defendants and the crucial factual basis for Plaintiff's CFAA claim: the alleged unauthorized access of her iPhone.

With regard to DarkMatter, only six paragraphs allege any connection between DarkMatter and the access of Plaintiff's device, and those are either explicitly based on "information and belief," *i.e.*, speculative (ECF 1 ¶¶ 104, 108-110, 112), or conclusory (*id.* ¶ 107). Plaintiff's failure to plead specific, non-conclusory facts dooms her claims against DarkMatter. *See Iqbal*, 556 U.S. at 679 ("[C]onclusions[] are not entitled to the assumption of truth.").

While the allegations regarding DarkMatter are facially speculative, those regarding the individual Defendants are entirely absent. The Complaint alleges zero factual basis for concluding that Baier, Adams, or Gericke participated in the alleged hacking of Plaintiff's iPhone. The Complaint alleges only that they worked for a U.S.-based company called CyberPoint, later worked for DarkMatter, developed the companies' alleged hacking capabilities, directed their hacking operations, and had inauthentic Apple accounts. (ECF 1 ¶¶ 7-9, 57-65, 67-73, 78, 84-86, 131-132.) While the allegations about their career paths and work are detailed, none implicates them in the tortious activity at the heart of this lawsuit: the alleged hacking of Plaintiff's phone. The Complaint additionally alleges that Baier, Adams, and Gericke entered into a deferred prosecution agreement based on their employment with CyberPoint and DarkMatter. (*Id.* ¶¶ 3, 7-9, 131-132.) But again, Plaintiff does not allege that the agreement concerns the alleged hacking of her phone. Indeed, the agreement makes no mention of Plaintiff. Her insinuation that the agreement somehow implicates Baier, Adams, and Gericke in the alleged hacking cannot save Plaintiff's claim from dismissal. *See Iqbal*, 556 U.S. at 678 ("Where a complaint pleads facts that are 'merely consistent with' a defendant's liability, it 'stops short of the line between possibility

and plausibility of 'entitlement to relief.'") (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 557 (2007)).

2. The CFAA Claim Fails To Meet the Statutory Requirements

Beyond failing to plead specific facts connecting any Defendant to the alleged hacking of Plaintiff's iPhone, Plaintiff fails to allege concrete facts that would satisfy any of the required statutory factors for a civil action under the CFAA. The CFAA authorizes a civil cause of action only if a person "suffers damage or loss by reason of a violation" of the statute, and that violation involves one of five factors specified in the statute. 18 U.S.C. § 1030(g). The CFAA defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information," *id*. § 1030(e)(8), and defines "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service," *id.* § 1030(e)(11). "The statutory definitions of 'damage' and 'loss' thus focus on technological harms—such as the corruption of files—of the type unauthorized users cause to computer systems and data." *Van Buren v. United States*, 141 S. Ct. 1648, 1660 (2021); *accord hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1195 n.12 (9th Cir. 2022) (quoting *Van Buren*). "Limiting 'damage' and 'loss' in this way makes sense in a scheme 'aimed at preventing the typical consequences of hacking.'" *Van Buren*, 141 S. Ct. at 1660 (quoting *Royal Truck & Trailer Sales & Serv., Inc. v. Kraft*, 974 F.3d 756, 760 (6th Cir. 2020)).

Plaintiff relies on the first and third factors: "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value," 18 U.S.C. § 1030(c)(4)(A)(i)(I); and "physical injury to any person," *id*. § 1030(c)(4)(A)(i)(III). (ECF 1 ¶ 139.) The allegations of the Complaint do not support either.

a. The Complaint Fails To Allege Facts Establishing A Loss Of At Least $5,000

To establish the first statutory factor, a plaintiff's losses "during any 1-year period [must] . . . aggregate[e] at least $5,000 in value." 18 U.S.C. § 1030(c)(4)(A)(i)(I). But the CFAA's definition of "loss" encompasses only "technological harms" and consequential damages resulting from interrupted service. *Van Buren*, 141 S. Ct. at 1660 (describing 18 U.S.C. § 1030(e)(11)). This definition of "loss" is "narrow," and establishes "limited parameters." *Andrews v. Sirius XM Radio Inc.*, 932 F.3d 1253, 1262-1263 (9th Cir. 2019).

Plaintiff's assertion that she suffered losses that amount to over $5,000 does nothing more than track the statutory standard: "Ms. Alhathloul suffered loss aggregating at least $5,000 in value. This loss includes costs incurred due to responding to the hack, conducting a damage assessment, and attempting to restore data." (ECF 1 ¶ 154.) That allegation provides no factual content that would support a reasonable inference that Plaintiff incurred costs that meet the statutory minimum. Such "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice" to state a claim. *Iqbal*, 556 U.S. at 678 (quoting *Twombly*, 550 U.S. at 555).

None of the Complaint's further allegations of loss meet the first statutory requirement, either. Plaintiff's alleged lost access to files is not quantified (ECF ¶ 156), so does not satisfy the value requirement. *See Brooks v. Agate Res., Inc.*, No. 6:15-CV-00983-MK, 2019 WL 2635594, at *24 (D. Or. Mar. 25, 2019), *report and recommendation adopted*, 2019 WL 2156955 (D. Or. May 14, 2019), *aff'd*, 836 F. App'x 471 (9th Cir. 2020) (plaintiff failed to allege loss of at least $5,000 where he failed to quantify alleged damages and failed to allege losses within meaning of CFAA). Nor do Plaintiff's alleged business and economic losses, which are not caused by interruption of service (ECF 1 ¶¶ 157, 159-160), fall within the "limited parameters" of the

statutory definition of loss. *See* 18 U.S.C. § 1030(e)(11) ("other consequential damages incurred *because of interruption of service*") (emphasis added); *Andrews*, 932 F.3d at 1263 ("[A]lthough the definition does include 'revenue lost,' that refers *only* to losses that occurred 'because of interruption of service.'"); *Brooks*, 2019 WL 2635594, at *24 (same); *contra Simmonds Equip., LLC v. GGR Int'l, Inc.*, 126 F. Supp. 3d 855, 865 (S.D. Tex. 2015) (lost business opportunity qualified as "consequential damages" because it resulted from an interruption in service).

The statutory definition also does not encompass replacement of family members' devices that are not alleged to have been accessed (ECF 1 ¶ 155), *see* 18 U.S.C. § 1030(e)(11) (defining "loss" as "any reasonable cost to any *victim* …") (emphasis added), and Plaintiff has not quantified the cost of those replacements in any event. Finally, Plaintiff's alleged loss of a vehicle (ECF 1 ¶ 158) falls outside the CFAA's definition of loss because does not reflect technological harm or consequential damages resulting from interrupted service, and was not directly caused by the alleged hacking. *Van Buren*, 141 S. Ct. at 1660; *Andrews*, 932 F.3d at 1263 ("The [CFAA's] 'loss' definition—with its references to damage assessments, data restoration, and interruption of service—clearly limits its focus to harms caused by computer intrusions, not general injuries unrelated to the hacking itself."); *Fraser v. Mint Mobile, LLC*, No. C 22-00138 WHA, 2022 WL 1240864, at *5 (N.D. Cal. Apr. 27, 2022) (holding that theft of cryptocurrency after cryptocurrency account was accessed through hacking of cell phone "does not constitute loss related to a computer or system," and "find[ing] that this type of damage or loss is not recognized by the CFAA") (citing *Andrews*, 932 F.3d at 1263).

Accordingly, this Court should dismiss the CFAA claim based on Plaintiff's insufficient "loss" allegations, as district courts regularly do in similar circumstances. *See, e.g., Andrews*, 932 F.3d at 1263 (affirming district court's denial of leave to amend complaint to assert CFAA claim

on futility grounds where alleged loss did not satisfy statutory definition); *Fraser*, 2022 WL 1240864, at *5 (dismissing CFAA claim because loss and damage not encompassed by CFAA definition); *Brooks*, 2019 WL 2635594, at *25 (dismissing CFAA claim for failure to allege loss covered by statutory definition, among other defects); *Ramirez v. SupportBuddy Inc.*, No. 17-cv-5781 (VB), 2018 WL 2089362, at *4 (S.D.N.Y. May 4, 2018) (dismissing CFAA claim because "plaintiff fail[ed] to quantify her alleged costs or make specific allegations as to the costs of repairing or investigating the alleged damage to her computer") (citing *Bose v. Interclick, Inc.*, No. 10-cv-9183 (DAB), 2011 WL 4343517, at *4 (S.D.N.Y. Aug. 17, 2011)); *Jensen v. Cablevision Sys. Corp.*, No. 17-cv-00100 (ADS)(AKT), 2017 WL 4325829, at *13 (E.D.N.Y. Sept. 27, 2017) (dismissing CFAA claim where plaintiff "fail[ed] to allege enough damages or loss to meet the [$5,000 minimum] requirement under the CFAA"); *Del Vecchio v. Amazon.com, Inc.*, No. C11-366 RSL, 2012 WL 1997697, at *4 (W.D. Wash. June 1, 2012) (same).

b. The Complaint Fails To Allege Facts Establishing Physical Injury

Plaintiff also argues that she suffered loss due to "physical injury to any person." 18 U.S.C. § 1030(c)(4)(A)(i)(III). That phrase is meant to encompass injury that is actually "caused (or, in the case of an attempted offense, would, if completed, have [been] caused)," by the statutory violation. *Id.* § 1030(c)(4)(B)(i). In other words, and consistent with the way "loss" is interpreted under the CFAA more broadly, the physical injury must stem from the unauthorized access itself, "not damages that flow from the *use* of unlawfully obtained information." *Fraser*, 2022 WL 1240864, at *5 (emphasis added); *see also Andrews*, 932 F.3d at 1263 (CFAA does not cover "general injuries unrelated to the hacking itself"); *Bank of Am. Corp. v. City of Miami*, 137 S. Ct. 1296, 1306 (2017) (observing that statutes that are "analogous" to common-law torts are subject to "directness principles" from common law, including "some direct relation between the injury asserted and the injurious conduct alleged"). Limiting covered physical injuries to those that are

a direct consequence of an unauthorized breach "makes sense in a scheme 'aimed at preventing the typical consequences of hacking.'" *Van Buren*, 141 S. Ct. at 1660 (quoting *Royal Truck*, 974 F.3d at 760).

This reading is supported by the legislative history, which evidences Congress' intent to cover physical injuries directly resulting from disruption of computers and computer networks. The Senate Report to the amendment of the CFAA adding "physical injury to any person" to the definition of "damage" explains that Congress was concerned about physical injury caused by interference with computers used in health and safety services:

> The bill addresses two other concerns [in addition to significant financial losses and potential impact on medical treatment]: causing physical injury to any person . . . and threatening the public health or safety . . . . As the [National Information Infrastructure] and other network infrastructures continue to grow, computers will increasingly be used for access to critical services such as emergency response systems and air traffic control, and will be critical to other systems which we cannot yet anticipate. Thus, the definition of 'damage' is amended to be sufficiently broad to encompass the types of harm against which people should be protected.

S. REP. No. 104-357, at 11 (1996).[4] Thus, when Congress added the phrase "physical injury to any person" to the statute, it did so "with a focus on the harm that the [CFAA] seeks to prevent," *id.*—namely, technological harms that directly cause physical injury. The term does not include injury resulting from misuse of information obtained via unauthorized access.

The physical injury Plaintiff alleges was not directly caused by the unauthorized access of any computer or network, and did not result from the alleged technological harm. Rather, the Complaint alleges that her physical injury was caused by an independent, intervening cause—namely, the Saudi security forces who allegedly harmed her. (ECF 1 ¶¶ 124-125, 130.) To be sure,

[4] Subsequent amendments moved the "physical injury to any person" factor, along with the other statutory factors, from the definition of "damage" to their present location at § 1030(c)(4)(A)(i). Pub. L. No. 110-326, § 204(a), 122 Stat. 3560 (2008); Pub. L. No. 107-56, § 814(a), 115 Stat. 272 (2001).

the Complaint alleges that the Saudi forces used information obtained through the alleged hacking to target and locate Plaintiff. (*Id*. ¶ 130.) But consequential physical injuries caused by independent actions of third parties who choose to commit heinous crimes like torture are unmistakably "damages that flow from the *use* of unlawfully obtained information," *Fraser*, 2022 WL 1240864, at *5 (emphasis added)—and thus are not harms the CFAA addresses.

B. Plaintiff's CFAA Conspiracy Claim (Count Two) Should Be Dismissed

Plaintiff's claim for conspiracy to violate the CFAA is also deficient, for two reasons. *First*, because Plaintiff's standalone CFAA claim fails, the conspiracy claim cannot survive either. *See Andersen v. Atlantic Recording Corp.*, No. 07-CV-934-BR, 2010 WL 1798441, at *4 (D. Or. May 4, 2010) (dismissing civil conspiracy claim where underlying claim failed) (citing *Oregon Laborers–Emp'rs Health & Welfare Tr. Fund v. Phillip Morris*, 185 F.3d 957, 969 (9th Cir. 1999)). Indeed, the Complaint is bereft of a single, non-conclusory allegation that the Defendants had an agreement to commit violations of the CFAA, as her CFAA conspiracy claim requires. *See Schmitz v. Mars, Inc.*, 261 F. Supp. 2d 1226, 1233 (D. Or. 2003).

Second, Plaintiff's CFAA conspiracy claim is barred by the intra-corporate conspiracy doctrine, which provides that "an agreement between or among agents of the same legal entity, when the agents act in their official capacities, is not an unlawful conspiracy." *Ziglar v. Abbasi*, 137 S. Ct. 1843, 1867 (2017). A fundamental element of a claim for conspiracy is an allegation of an agreement between two or more persons. *Schmitz*, 261 F. Supp. 2d at 1233. Because a corporation, its agents, and employees are considered a single entity, however, "concerted action by officers within a single corporate entity cannot give rise to liability for conspiracy." *Cool Runnings Int'l Inc. v. Gonzalez*, No. 1:21-CV-00974-DAD-HBK, 2021 WL 5331453, at *14 (E.D. Cal. Nov. 16, 2021) (dismissing claim for conspiracy to violate CFAA).

Plaintiff asserts a claim for conspiracy against Defendants DarkMatter, Baier, Gericke, and Adams. (ECF 1 ¶ 166.) But Plaintiff alleges that the three individual defendants are DarkMatter employees (*see id*. ¶ 1), and that all relevant acts were taken within the scope of their employment. For instance, Defendants are alleged to have participated in a "cyber-surveillance program known as Project Raven" that was "operated" by DarkMatter. (*Id*. ¶ 6.) Plaintiff alleges that "Defendants Baier, Adams, and Gericke supported, directed, and supervised DarkMatter in creating the Karma hacking system" that forms the basis of Plaintiff's claims. (*Id*. ¶ 85.) And she alleges that Defendants are liable for their actions "arising out of their conduct while employees" at DarkMatter. (*Id*. ¶ 131.) Because these Defendants cannot conspire with each other as a matter of law, Plaintiff's conspiracy claim should be dismissed. *See, e.g.*, *Cool Runnings*, 2021 WL 5331453, at *14; *Hunt v. City of Portland*, No. CV 08-802-AC, 2008 WL 11389551, at *9 (D. Or. Nov. 19, 2008), *report and recommendation adopted*, 2008 WL 11389544 (D. Or. Dec. 18, 2008) (dismissing claims and noting that "[t]he intracorporate conspiracy exception, which originated in the antitrust arena, provides that employees are deemed incapable of conspiring among themselves or with their employer when they are acting as agents of the employer"); *Hoefer v. Fluor Daniel, Inc.*, 92 F. Supp. 2d 1055, 1058 (C.D. Cal. 2000) (dismissing statutory claims under the intra-corporate conspiracy doctrine).

III. PLAINTIFF'S ATS CLAIM (COUNT THREE) SHOULD BE DISMISSED

Plaintiff brings a claim for violation of the Alien Tort Statute ("ATS") against the individual Defendants only, alleging that they engaged in "persecution" (an alleged crime against humanity) by acting as agents of DarkMatter in hacking the electronic devices of Plaintiff and others not before the court. (ECF 1 ¶ 172.) The Court should dismiss this claim for lack of subject matter jurisdiction. *See* FED. R. CIV. P. 12(b)(1); *Nestlé USA, Inc. v. Doe*, 141 S. Ct. 1931, 1936 (2021) (ATS is "purely jurisdictional"). That is so for two independent reasons: (1) Plaintiff's allegations

concern entirely extraterritorial conduct; and (2) they do not describe a violation of a recognized norm of international law.

First, Plaintiff impermissibly seeks extraterritorial application of the ATS. Conduct that occurs entirely or primarily abroad is beyond the scope of the statute. *See Kiobel v. Royal Dutch Petroleum Co.,* 569 U.S. 108 (2013) (holding that ATS claims are subject to the presumption against extraterritoriality); *see, e.g.*, *Hmong I v. Lao People's Democratic Republic*, 748 F. App'x 136, 137 (9th Cir. 2019) (affirming dismissal of complaint for lack of jurisdiction because "Plaintiff did not allege any domestic conduct"); *Balintulo v. Daimler AG*, 727 F.3d 174, 190 (2d Cir. 2013) ("[I]f all the relevant conduct occurred abroad, that is simply the end of the matter."). "[E]ven where the claims touch and concern the territory of the United States" in some manner, "they must do so with sufficient force to displace the presumption against extraterritorial application." *Kiobel*, 569 U.S. at 124-125. In other words, an ATS plaintiff must plead domestic conduct that is relevant to the "focus" of the statute; peripheral or incidental domestic conduct is not enough. *Nestlé*, 141 S. Ct. at 1936-1937; *see id.* at 1935 (no ATS jurisdiction even though "defendant corporations allegedly made 'major operational decisions' in the United States").

Plaintiff seeks an impermissible extraterritorial application of the ATS. All alleged events that are the "focus" of the ATS claim of "persecution" took place in the UAE or Saudi Arabia: Plaintiff was allegedly arrested in the UAE and harmed in the UAE and Saudi Arabia. (ECF 1 ¶¶ 20, 25-27, 116-123.) All of Defendants' conduct is alleged to have occurred overseas as well, in the UAE. Indeed, the Complaint alleges no U.S.-based *conduct* at all (other than the fortuitous alleged contacts with U.S.-based servers described above). (*Id.* ¶ 105.) These allegations fall far outside of the permissible territorial scope of the ATS and require dismissal. *See, e.g.*, *Nestlé*, 141 S. Ct. at 1937; *Doe I v. Cisco Sys., Inc.*, 66 F. Supp. 3d 1239, 1242 (N.D. Cal. 2014) (dismissing

ATS claims on extraterritoriality grounds, despite allegations that defendants directed and planned activities in San Jose, California, with "the primary goal of creating an online surveillance system to enable and facilitate the suppression of dissident activity" abroad).

Second, Plaintiff's ATS claim should also be dismissed because the facts that Plaintiff alleges give rise to "persecution" do not constitute a recognized tort on which an ATS claim may be based. Traditionally, ATS claims encompassed only three underlying torts that were widely accepted under international law when the ATS was created: violation of safe conducts, infringement of the rights of ambassadors, and piracy. *Sosa v. Alvarez–Machain*, 542 U.S. 692, 724 (2004). Efforts to expand this list are both generally disfavored and closely scrutinized. Accordingly, ATS liability is reserved for a "narrow set" of customary international law norms that are "specific, universal, and obligatory" and have "definite content and acceptance among civilized nations." *Id*. at 721, 724, 729-732.

As courts interpreting the ATS have warned, "[t]he ATS is no license for judicial innovation." *Mamani v. Berzain*, 654 F.3d 1148, 1152 (11th Cir. 2011). Instead, "federal courts must act as vigilant doorkeepers and exercise great caution when deciding either to recognize new causes of action under the ATS or to broaden existing causes of action." *Id*. (citing *Sosa*, 542 U.S. 692); *Moskovits v. Mercedes-Benz USA, LLC*, No. 1:21-CV-20122-JEM/Becerra, 2022 WL 283001, at *18 (S.D. Fla. Jan. 10, 2022), *report and recommendation adopted*, 2022 WL 278959 (S.D. Fla. Jan. 31, 2022) (dismissing ATS claim premised on violation of the Universal Declaration of Human Rights because plaintiff failed to allege that defendant "violated established international law"). To do so, "courts should require any claim based on the present-day law of nations to rest on a norm of international character accepted by the civilized world and defined

with a specificity comparable to the features of the 18th-century paradigms we have recognized." *Sosa*, 542 U.S. at 725. Failure to do so is "fatal" to an ATS claim. *Id*.

Plaintiff seeks to bring her ATS claim based on the individual Defendants' alleged conspiracy to commit, or aid and abet, the crime of "persecution." (ECF 1 ¶¶ 173-174.) She alleges that this persecution has taken the form of a "systematic or widespread attack on [a] civilian population" of "perceived dissidents of the UAE and Saudi Arabia" to include "hacking the devices and tracking the locations of members of the persecuted group; stealing their personal information; imposing travel bans; and subjecting them to arbitrary arrests and detention, sham trials, torture, enforced disappearances, extrajudicial killings, as well as harassment and abuse of their family members." (*Id.* ¶ 172.) As these claims pertain to her, Plaintiff essentially claims that the UAE (through the individual Defendants, acting as the UAE's supposed agents) used technology to spy on her while she was physically present in the UAE.

Even accepting those allegations as true, however, she cannot show that they amount to a violation of "established international law," *i.e.*, "a norm of international character accepted by the civilized world and defined with a specificity comparable to the features of the 18th-century paradigms [the Supreme Court has] recognized," such as piracy. *Sosa*, 542 U.S. at 725. Indeed, no court has ever found that the sorts of activities carried out by the individual Defendants—allegedly assisting a foreign sovereign's surveillance of foreigners—constitutes an actionable ATS claim. With good reason: accepting those allegations as sufficient would require opining as to the legality of the sovereign activities of a foreign country taken on its own soil. *See Broidy Cap. Mgmt., LLC v. State of Qatar*, 982 F.3d 582, 592 (9th Cir. 2020) ("The status of peacetime espionage under international law is a subject of vigorous debate[.]"), *cert. denied sub nom. Broidy Cap. Mgmt., LLC v. Qatar*, 141 S. Ct. 2704 (2021); *Doe I v. Cisco Sys., Inc.*, No. 5:11-CV-02449-

EJD, 2015 WL 5118004, at *4 (N.D. Cal. Aug. 31, 2015) (refusing to disturb dismissal of ATS claims and noting that the "manner in which the Chinese Government chooses to enforce its laws is a political question that is better suited for our executive and legislative branches of government").

In any event, Plaintiff's factual allegations—which concern only herself and three other individuals (ECF 1 ¶¶ 74, 76-77)—would hardly constitute the sort of "sufficiently widespread—or . . . sufficiently systematic" conduct that could "amount definitely to a crime against humanity under already established international law." *Mamani*, 654 F.3d at 1156 (dismissing allegations that 70 people were killed and 400 were injured over a period of two months as insufficient to allege the crime against humanity of extrajudicial killings). Thus, even if "persecution" in the form of assisting a foreign sovereign's electronic surveillance on foreign soil were a recognized basis of ATS liability, her ATS claim would still fail.

IV. PLAINTIFF'S AGENCY ALLEGATIONS, IF ACCEPTED AS TRUE, RENDER DEFENDANTS IMMUNE FROM SUIT

Plaintiff alleges that all of the Defendants acted as agents of the UAE, *i.e.*, that Defendants' alleged actions were "for use against her by the security services of the [UAE]." (ECF 1 ¶ 1.) The Complaint devotes two sections of its Statement of Facts to allegations that the UAE "utilized" Defendants to target human rights activists. (*Id.* ¶¶ 60-77). And Plaintiff claims that her iPhone was hacked as "part of the UAE's campaign of persecution against perceived dissidents of itself and Saudi Arabia." (*Id.* ¶ 113). In other words, Plaintiff alleges that Defendants acted as agents of the UAE—*i.e.*, "on the [UAE's] behalf and subject to the [UAE's] control." RESTATEMENT (THIRD) OF AGENCY § 1.01; *see Willis v. Nationwide Debt Settlement Grp.*, No. 3:11-CV-430-BR, 2012 WL 13055512, at *4 (D. Or. May 22, 2012) ("[T]o be an 'agent'—using the well-defined legal meaning of that term—two requirements must be met: (1) the individual must be subject to

another's control; and (2) the individual must 'act on behalf of' the other person.") (quoting *Vaughn v. First Transit, Inc*., 346 Or. 128, 136 (2009)).

If Plaintiff's agency allegations are accepted as true—as they must be on a motion to dismiss—Defendants are entitled to common law conduct-based immunity. *Samantar v. Yousuf*, 560 U.S. 305, 321 (2010) (recognizing that common-law conduct-based immunity is afforded to an "agent of [a foreign] state with respect to acts performed in his official capacity if the effect of exercising jurisdiction would be to enforce a rule of law against the state") (emphasis added). As other circuits have recognized, even private entities acting at the direction of a foreign state may be entitled to immunity from liability under common-law immunity principles. *Butters v. Vance Int'l, Inc*., 225 F.3d 462, 466 (4th Cir. 2000) (recognizing derivative sovereign immunity under Foreign Sovereign Immunities Act for private contractor, while applying common-law immunity principles); *Broidy Cap. Mgmt. LLC v. Muzin*, 12 F.4th 789, 802 (D.C. Cir. 2021) (considering common-law immunity claim of private contractor working for a foreign state, but ultimately finding no immunity available based on facts).[5] Such conduct-based immunity presents yet another independent ground for dismissal.

CONCLUSION

For the foregoing reasons, the complaint should be dismissed.

[5] DarkMatter acknowledges that this argument is currently unavailable to DarkMatter under *WhatsApp Inc. v. NSO Group Technologies Limited*, 17 F.4th 930, 940 (9th Cir. 2021), which concluded that the Foreign Sovereign Immunities Act, rather than common-law immunity, governs the sovereign immunity of non-natural persons. DarkMatter is therefore preserving the argument in light of the petition for certiorari filed by the appellees in *WhatsApp*. Pet. for Writ of Cert., *NSO Grp. Technologies Ltd. v. WhatsApp Inc*., No. 21-1338 (Apr. 8, 2022).

Respectfully submitted,

Dated: May 31, 2022

SCHWABE, WILLIAMSON & WYATT, P.C.

s/ Nika Aldrich
Nika Aldrich, OSB No. 160306
Telephone: 503-222-9981

AKIN GUMP STRAUSS HAUER & FELD LLP

s/ Anthony T. Pierce
Anthony T. Pierce (*pro hac vice*)
Caroline L. Wolverton (*pro hac vice)*
Telephone: (202) 887-4000

Natasha G. Kohne (*pro hac vice*)
Telephone: (415) 765-9500

ATTORNEYS FOR DEFENDANT DARKMATTER GROUP

SNELL & WILMER L.L.P.

s/ Clifford S. Davidson
Clifford S. Davidson, OSB No. 125378
Telephone: 503-624-6800

ATTORNEY FOR DEFENDANTS MARC BAIER, RYAN ADAMS, AND DANIEL GERICKE