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
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
100 Pine St., Suite 3200
San Francisco, CA 94111
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

(Complete list of counsel appears on signature page)

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' JOINT MOTION TO DISMISS FIRST AMENDED COMPLAINT** **REQUEST FOR ORAL ARGUMENT**

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

LOCAL RULE 7-1 CERTIFICATION

The undersigned counsel hereby certifies that on July 6, 2023, counsel discussed the substance of this Motion with counsel for Plaintiff. The parties were unable to resolve the dispute.

MOTION

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

INTRODUCTION

Plaintiff Loujain Hathloul Alhathloul's second attempt to establish personal jurisdiction over foreign defendants in this Court fares no better than the first. This Court dismissed Plaintiff's original complaint against DarkMatter (a United Arab Emirates company with no U.S. presence) and three former DarkMatter employees (who all reside abroad) for two overarching reasons. *First*, Defendants lack the requisite "minimum contacts" with the United States because their alleged conduct of sending iMessages (from abroad) containing malware to Plaintiff's iPhone (located abroad) was not "purposefully directed" at the United States, and Plaintiff could not rely on Defendants' U.S. contacts that did not give rise or relate to her claims. *Second*, exercising jurisdiction would be unreasonable given the foreign nature of the parties, the claimed harm, and potential evidence and witnesses, as well as the fact that Plaintiff's claims implicated the sovereign interests of foreign nations.

Plaintiff's Amended Complaint has the same deficiencies. Plaintiff seeks to strengthen her ties to the United States by alleging that she had connections with various U.S. journalists and non-governmental organizations, and that she traveled to the United States after her phone was allegedly hacked. But it is well established that a plaintiff's unilateral contacts with the forum cannot establish minimum contacts. Plaintiff's additional allegations regarding underlying technology and communications with persons who happen to have connections to the United States

cannot establish that Defendants' alleged conduct targeted the United States, either. And allegations concerning Defendants' general (not claim-specific) connections to the United States play no role in the minimum contacts analysis, as this Court's prior decision makes clear. In any event, Plaintiff's new allegations do nothing to displace this Court's finding that exercising jurisdiction over Defendants would be unreasonable.

Alternatively, on the merits, Plaintiff fails to state any plausible claim for relief. Plaintiff's Computer Fraud and Abuse Act ("CFAA") claim should be dismissed because the statute does not reach the wholly foreign conduct alleged here. In addition, Plaintiff's "information and belief" allegations fail to connect any of the Defendants to the alleged hacking of Plaintiff's phone, nor can they satisfy the statutory "loss" standard. Plaintiff's conspiracy claim under the CFAA is also barred—not only because the underlying claim is deficient, but also pursuant to the act of state doctrine, because a finding in Plaintiff's favor would require the Court to conclude that actions of alleged co-conspirator government officials, taken on their own soil, were unlawful. And this Court lacks jurisdiction over Plaintiff's claim under the Alien Tort Statute ("ATS").

Because Plaintiff's second attempt to establish personal jurisdiction and state plausible claims for relief again falls short, the Court should dismiss Plaintiff's Amended Complaint—this time with prejudice.

BACKGROUND

In her original complaint, Plaintiff alleged that, in late 2015 or early 2016, the UAE government retained Defendant DarkMatter, a UAE company, to provide cybersecurity services. (*See* ECF 1 ¶¶ 6, 67.) Defendants Marc Baier, Ryan Adams, and Daniel Gericke, who had previously worked for a U.S. company in the UAE that provided similar services for the UAE government, joined DarkMatter as employees. (*See id.* ¶ 69.) Plaintiff alleged that, at some point before March 2018, DarkMatter hacked (from the UAE) her iPhone (located in the UAE) by

sending an "iMessage" to Plaintiff's "Messages" application. (*See id.* ¶¶ 87-104.) She alleged 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.) Plaintiff asserted claims against all Defendants for violating and conspiring to violate the CFAA, and a claim against Baier, Adams, and Gericke under the ATS. (*Id.* ¶¶ 134-177.)

This Court dismissed Plaintiff's claims for lack of personal jurisdiction because Plaintiff's allegations failed all three mandatory steps of the due process inquiry. (*See* ECF 44 at 20.)

First, "Defendants did not purposefully direct their actions at the United States." (ECF 44 at 9 (formatting modified).) The Court applied that "purposeful direction" test because Defendants' "allegedly tortious conduct took place outside of the forum." (*Id.* at 10.) Both "the location where the Defendants sent the message" and "the location that contain[ed] the hardware," i.e., Plaintiff's phone when it allegedly "receive[d] and processe[d] the attacker's message," had been located abroad. (*Id.* (internal quotation marks omitted).) Applying the purposeful direction test, the Court held that "Defendants' use of Apple's U.S.-based servers [did] not constitute express aiming at the United States." (*Id.* at 12 (formatting modified).) The fact that iMessages traversed those servers, "at most, shows Defendants purposefully directed their conduct at a third party—Apple, whose choice to host their servers in the United States is entirely unrelated to the conduct at issue[.]" (*Id.* at 13.) Further, Plaintiff's allegations did "not support the inference that Defendants knew that harm was likely to be suffered [by Plaintiff] in the United States as opposed to some other forum." (*Id.* at 16-17.)

Second, "Plaintiff's claims [did] not arise out of or relate to Defendants' forum-related activities." (ECF 44 at 18 (formatting modified).) Here again, Plaintiff's theory based on Apple's servers relied on a "third party's contacts with the United States," not Defendants' alleged contacts.

(*Id.*) And while Plaintiff had also relied on Defendants' alleged "acquisition of exploits, reliance on U.S. technology and knowhow … , employment of U.S. individuals, and U.S. anonymization services," Plaintiff had "failed to plead with sufficient specificity how this background conduct relate[d] to the use of specific malware to infect Plaintiff's phone," particularly because the technology was "altered in significant ways before being deployed in the hack[.]" (*Id.* at 19.) More generally, "the fact that Defendants may have developed expertise and knowhow in the forum that was later used to create the malware … is not enough to confer jurisdiction." (*Id.*)

Third, "[e]ven if Plaintiff had shown that Defendants had sufficient 'minimum contacts' with the United States," the Court found "that the exercise of jurisdiction over Defendants would be unreasonable." (ECF 44 at 20.) Defendants' alleged conduct "present[ed] no 'purposeful interjection' into United States' affairs"; Plaintiff's allegations implicated "the sovereignty of … the UAE government"; the United States had little "interest in adjudicating the dispute" because "Plaintiff is not a United States resident"; and "the United States would not offer the most efficient judicial resolution for the controversy" given "the almost completely foreign nature of the tortious conduct at issue" and because the "relevant parties, documents, and witnesses" were located abroad. (*Id.* at 20, 21, 22.)

Plaintiff's Amended Complaint asserts the same claims based on largely the same allegations. Plaintiff's new allegations include that, after she was hacked sometime "in 2017" (ECF 54 at ¶ 134), Defendants "exfiltrated … data from [her] device while she was physically present in the United States" because Plaintiff traveled to the United States to attend several events "during th[e] period of surveillance." (*Id.* ¶¶ 24-28, 143-150.) Plaintiff alleges that a Saudi Arabian "charging document … referenced" some of those U.S. activities. (*Id.* ¶ 170.) And Plaintiff purports to allege more details regarding Defendants' acquisition and use of U.S.

technology. (*See id.* ¶¶ 94-103, 107 (alleging Defendants purchased "exploit[s]" from a U.S. company and "were in direct contact with the U.S. company about how to configure [the exploits] into a hacking system," and used "a U.S. company's anonymization services and proxy servers to prevent detection").) Finally, although Plaintiff previously relied heavily on the individual Defendants' Deferred Prosecution Agreement (DPA) with the U.S. Department of Justice, she now incorporates by reference that document (and the individual Defendants' consent agreements with the U.S. Department of State) into her Amended Complaint. (*See id.* ¶¶ 3, 175-177, Exs. A & B.) DarkMatter is not a party to those agreements, nor do those agreements reference Plaintiff.

ARGUMENT

I. THE COURT LACKS PERSONAL JURISDICTION OVER ALL DEFENDANTS

This Court still lacks personal jurisdiction over any Defendant. Having failed to establish jurisdiction based on a third party's contacts (i.e., the location of Apple's servers), Plaintiff seeks to do so based on her own contacts (i.e., her travel to the United States) and those of additional third parties (i.e., companies that allegedly supplied DarkMatter with technology). But only *Defendants'* claim-specific contacts count, and Plaintiff does not allege that Defendants targeted the United States or knew their conduct was likely to cause harm there. Nor do Plaintiff's new allegations upset the Court's prior determination that exercising jurisdiction over Defendants would be unreasonable.

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 Techs, Inc.*, 647 F.3d 1218, 1223 (9th Cir. 2011). To establish jurisdiction under Rule 4(k)(2), a plaintiff must (i) bring a federal claim, (ii) show that the defendant is not "subject to the personal jurisdiction of any state court of general

jurisdiction," and (iii) demonstrate 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). Under Rule 4(k)(2), courts "consider contacts with the nation as a whole" rather than contacts with the forum state. *AMA Multimedia, LLC v. Wanat*, 970 F.3d 1201, 1208 (9th Cir. 2020) (quoting *Holland Am. Line*, 485 F.3d at 462).

For specific jurisdiction, "[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 notice of fair play and substantial justice.'" *AMA*, 970 F.3d at 1208 (quoting *Int'l Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945)). Specifically, a plaintiff must satisfy three elements:

1) The non-resident defendant must purposefully direct his activities or consummate some transaction with the forum or 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

Plaintiff cannot satisfy any prong of the due process inquiry.

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

Under the first prong, "[c]ourts apply the purposeful direction analysis, also known as the 'effects test,' to conduct that occurs outside of the forum … but whose effects are felt within the forum." (ECF 44 at 8 (citing *Freestream*, 905 F.3d at 605)); *see AMA*, 970 F.3d at 1208 (effects test applies when "allegedly tortious conduct takes place *outside* the forum" and allegedly "has

effects inside the forum" (citing *Calder v. Jones*, 465 U.S. 783 (1984))). This Court already found "that the purposeful direction test provides the proper framework for analyzing Defendants' jurisdictional challenge." (ECF 44 at 12.) Plaintiff does not allege that Defendants took any "deliberate action within the forum" or performed any of "the liability-producing acts while physically present" there. *Freestream*, 905 F.3d at 604, 606.[1]

Under the effects test, "the defendant allegedly must have (1) committed an intentional act, (2) expressly aimed at the forum … , (3) causing harm that the defendant knows is likely to be suffered in the forum[.]" *AMA*, 970 F.3d at 1209 (quotation 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*, 571 U.S. at 284, 286. "[T]he relationship must arise out of contacts that the 'defendant *himself*' creates with the forum[.]" *Id.* at 284. Although Plaintiff alleges an intentional act, she fails to allege that DarkMatter either expressly aimed any tortious conduct at the United States or caused harm it knew would likely be suffered there.

[1] Although this Court's prior order left open whether "the location that contain[ed] the hardware manipulated by the defendant[s]" is relevant to where the tortious conduct occurred (ECF 44 at 10), Ninth Circuit precedent requires examining the location of the alleged "tortfeasors," *Freestream*, 905 F.3d at 605-606 ("effects test" gauging the nexus between the alleged conduct and the forum "makes more sense" for alleged "out-of-forum tortfeasors" (internal quotation marks omitted)); *accord Will Co., Ltd. v. Lee*, 47 F.4th 917, 921-922 (9th Cir. 2022) (applying "effects test" to tortfeasors located abroad even though copyrighted material was hosted on U.S. servers and viewed over one million times on U.S. devices). Indeed, in *Calder* itself (from which the "effects test" derives), the Supreme Court looked to the "'effects' of [defendants'] Florida conduct in California," *Calder*, 465 U.S. at 789, even though the tort "actually occurred in California," *Walden v. Fiore*, 571 U.S. 277, 287-288 (2014) (noting that "libel is generally held to occur wherever the offending material is circulated"). Regardless, "the allegedly tortious conduct took place outside of the forum" either way because "Defendants began their tort of knowingly transmitting malware in a foreign country," and the malware allegedly "activated on the target's phone … outside of the forum." (ECF 44 at 10-11); *cf. Walden*, 571 U.S. at 288-289 (where defendant "never traveled to, conducted activities within, contacted anyone in, or sent anything or anyone to [the forum]," "no part of [defendant]'s course of conduct occurred [there]").

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

Plaintiff has not plausibly alleged that DarkMatter "aim[ed]" any intentional tort-related conduct at the United States. *See AMA*, 970 F.3d at 1209 n.5. Although much of her Amended Complaint still relates to DarkMatter's alleged contacts with a third party's servers, this Court has already held that "Defendants' use of Apple's U.S.-based servers does not constitute express aiming at the United States" because "the location of Apple's servers in the United States is 'fortuitous.'" (ECF 44 at 12-13 (citing, *e.g.*, *Hungerstation LLC v. Fast Choice LLC*, 857 F. App'x 349, 351 (9th Cir. 2021)).) Indeed, 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. Although Plaintiff now alleges that DarkMatter employees knew that "the exploits relied on Apple's U.S.-based servers" (ECF 54 ¶ 132), "[m]ere knowledge of the location of a third party's servers … is not sufficient to constitute purposeful direction." (ECF 44 at 16.) That is certainly true where, as here, Plaintiff's allegations regarding Apple's servers are just hyper-technical descriptions of Apple's processes triggered by *anyone* who sends an iMessage to an iPhone located anywhere in the world.[2]

[2] *Compare* ECF 54 ¶¶ 113, 114 (alleging DarkMatter "retriev[ed]" Plaintiff's "encryption and routing information from Apple's identity servers," "encrypt[ed] the iMessage," 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"). Defendants request that the Court take judicial notice of Apple's publicly posted technical information under Rule 201(b)(2) of the Federal Rules of Evidence.

Because DarkMatter's contacts with Apple have already been ruled insufficient, Plaintiff's Amended Complaint relies on two new forum-related contacts. *First*, Plaintiff relies on her *own* contacts with the forum—specifically, the fact that she voluntarily traveled to the United States with her phone after it was hacked, which allegedly allowed DarkMatter to "exfiltrate[] … data from [her] device while she was physically present in the United States." (ECF 54 ¶ 150.) But "the 'unilateral activity' of a plaintiff" cannot support jurisdiction. *Walden*, 571 U.S. at 286 (quoting *Burger King v. Rudzewicz*, 471 U.S. 462, 475 (1985)). Subjecting a defendant to jurisdiction based on a plaintiff's movements would thwart the defendant's ability to "'structure [its] primary conduct' to lessen or avoid exposure to a [forum]'s courts." *Ford Motor Co. v. Mont. Eighth Judicial Dist. Court*, 141 S. Ct. 1017, 1025 (2021) (quoting *World-Wide Volkswagen Corp. v. Woodson*, 444 U.S. 286, 297 (1980)). Thus, a plaintiff's mere allegation that she "suffered [an] injury caused by [the defendant's] allegedly tortious conduct … while … in the forum" does not establish express aiming. *Walden*, 571 U.S. at 289. "Regardless of where a plaintiff" is located, the plaintiff's "injury is jurisdictionally relevant only insofar as it shows that *the defendant* has formed a contact with the forum," i.e., that "the defendant's conduct connects him to the forum in a meaningful way." *Id.* at 290 (emphasis added). For example, in *Walden*, Nevada lacked personal jurisdiction over the defendants even though the plaintiffs' injuries "foreseeabl[y]" occurred there: Nevada was merely "where [the plaintiffs] chose to be at [the] time" of the injuries, and they "would have experienced this same [harm] … wherever else they might have traveled." *Id.* at 289, 290.

The same is true here. Plaintiff alleges that DarkMatter tortiously sent an iMessage containing malware to Plaintiff while she was located abroad, and that she later suffered some harm (i.e., transmission of personal data) while she was located in the United States. That is not

an allegation that DarkMatter deliberately aimed its conduct at the United States, but rather that DarkMatter's conduct affected the United States solely due to Plaintiff's voluntary travel choices. Given Plaintiff's allegation that her "compromised [device] … continuously transmit[ted] data" to Defendants' servers (ECF 54 ¶ 127), Plaintiff would have experienced the same harm "wherever else [she] might have traveled." *Walden*, 571 U.S. at 290.

Second, Plaintiff points again to DarkMatter's supposed contacts with additional U.S.-based third parties beyond Apple, including DarkMatter's alleged choice to "rout[e] … communications through U.S.-based anonymization services and other proxy servers hosted in the United States to prevent detection and attribution," acquisition of "exploits" from two American companies, and communications with those companies regarding "how to configure" the exploits "into a hacking system." (ECF 54 ¶¶ 93, 97, 103, 105, 107-108.) Plaintiff emphasized the same points at the hearing on Defendants' first motion to dismiss. (*See* ECF 45 at 24:22-24:4.) Even accepting "as true" the allegation that Defendants intentionally and "specifically targeted" such third parties, those allegations still "do not create the type of contact between the United States and *Defendants' conduct* that could give rise to personal jurisdiction," because they do not show that DarkMatter directed its "conduct at the forum." (ECF 44 at 13 (emphasis added)); *see AMA*, 970 F.3d at 1212 (similar allegations "do[] not show targeting of the" United States).

For example, in *AMA*, the Ninth Circuit rejected the argument that a defendant's use of "an American domain name server … that allow[ed]" U.S.-based users to access the defendant's website more efficiently "evidence[d] targeting." 970 F.3d at 1212. Although the defendant had obviously used the services of a U.S. company, there was no indication that the defendant "was motivated by a desire to appeal to the U.S. market or generate more U.S. users[.]" *Id.* Beyond

AMA, other courts have found "no personal jurisdiction where the plaintiff alleged that the defendants used U.S.-based web server companies to host purportedly infringing content." (*See* ECF 44 at 14 (citing *42 Ventures, LLC v. Mav*, No. 20-17305, 2021 WL 5985018, at *1 (9th Cir. Dec. 16, 2021)).) Here, there is likewise no allegation (or indication) that DarkMatter worked with companies or technologies because of their alleged links to the United States—let alone because of a desire to aim any tortious conduct at the United States. Instead, they show "at most" that DarkMatter "purposefully directed [some] conduct at … third part[ies]" whose connections to the United States, like Apple's, are "entirely unrelated to the conduct at issue in Plaintiff's complaint." (ECF 44 at 13.)

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

Plaintiff's failure to point to any "harm" that DarkMatter "knew" "was likely to be suffered in the United State[s] as opposed to some other forum" remains an independent basis for dismissal. (ECF 44 at 17); *see AMA*, 970 F.3d at 1209 (defendant must "know" that harm is "likely to be suffered in" forum); *Brown v. Serv. Grp. of Am., Inc.*, No. 3:20-cv-2205-IM, 2022 WL 43880, at *3 (D. Or. Jan. 5, 2022) (Immergut, J.), *aff'd*, No. 22-35107, 2022 WL 16958933 (9th Cir. Nov. 16, 2022) (dismissing complaint for failure to establish defendant knew harm would likely be suffered in Oregon); *Traeger Pellet Grills, LLC v. Deadwood Biofuels, LLC*, No. 3:11-cv-01221-JE, 2012 WL 4040211, at *5 (D. Or. June 21, 2012), *report and recommendation adopted*, 2012 WL 4039848 (D. Or. Sept. 11, 2012) (same). "[T]he focus for this element of the jurisdictional analysis must be on the foreseeability of harm caused in the forum to the plaintiff, not to a third party not otherwise involved in the litigation." (ECF 44 at 17.)

Plaintiff does not allege that DarkMatter engaged in any conduct vis-à-vis Plaintiff while she was located in the United States or targeted her *because* she would be traveling there. *See*

Brown, 2022 WL 43880, at *3 ("[T]he harm prong requires that the defendant's actions be 'performed for the very purpose of having their consequences felt in the forum state.'" (quoting *Brainerd v. Governors of the Univ. of Alberta*, 873 F.2d 1257, 1260 (9th Cir. 1989))). Plaintiff alleges that she voluntarily took a trip to the United States, which was publicized on social media (ECF 54 ¶¶ 144-146), and speculates that her phone was monitored during the trip based on an earlier hacking incident. But that is not a specific allegation that DarkMatter even knew about the trip, let alone "knew that harm was likely to be suffered in the United State[s] as opposed to some other forum." (ECF 44 at 17.) And even if DarkMatter *did* know, "knowledge of [a plaintiff's] strong forum connections … combined with [the] conclusion that [the plaintiff] suffered foreseeable harm in" the forum does not "satisf[y] the 'minimum contacts' inquiry." *Walden*, 571 U.S. at 289. Permitting jurisdiction on that basis would "impermissibly allow[] a plaintiff's contacts with the defendant and forum to drive the jurisdictional analysis." *Id*. And Plaintiff's vague and conclusory allegation that "[t]he hacking was intended to provide constant surveillance of [her] communications with other human rights advocates, researchers, and journalists, including U.S.-based" persons (ECF 54 ¶ 140), neither indicates that DarkMatter *knew* the persons were based in the United States nor relates to the "foreseeability of harm caused *in the forum* to the *plaintiff*." (ECF 44 at 17 (emphasis added).)

In any event, the United States is plainly not "the focal point … of the harm suffered." *AMA*, 970 F.3d at 1212 (quoting *Walden*, 517 U.S. at 287; *Calder*, 465 U.S. at 789). "A defendant causes harm in a particular forum when the 'bad acts' that form the basis of the plaintiff's complaint occur in that forum." (ECF 44 at 16 (quoting *Will Co.*, 47 F.4th at 926).) But no specific "bad acts" are alleged to have occurred in the United States: Plaintiff alleges that the hacking occurred before her voluntary U.S. visit, and simply speculates (on "information and belief") that she may

have been monitored while in the United States. (ECF 54 ¶ 150.) Plaintiff further alleges that DarkMatter intended to provide information to foreign governments, that she suffered the consequences of the hacking in Saudi Arabia and the UAE, and that in fact she "did not discover" any alleged hack "until she became aware of … reporting by *Reuters*" long after leaving the United States. (*Id.* ¶ 155; *see also id.* ¶¶ 156-171.) Thus, any nebulous harm that Plaintiff experienced based on the alleged exfiltration of her data while she happened to be present in the United States was not "jurisdictionally sufficient" (ECF 44 at 16), because it was not "*felt* … within" the forum, *see Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme*, 433 F.3d 1199, 1206 (9th Cir. 2006) (en banc) (emphasis added); *see also Dole Food Co. v. Watts*, 303 F.3d 1104, 1111 (9th Cir. 2002) (harm must be jurisdictionally "significant").

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). "[F]or an injury to *arise out of* a defendant's forum contacts requires but for causation," i.e., "a direct nexus … between a defendant's contacts with the forum … and the cause of action." *Yamashita v. LG Chem, Ltd.*, 62 F.4th 496, 504 (9th Cir. 2023) (emphasis added) (alterations and internal quotation marks omitted). "*[R]elate to*," while broader, "does not mean anything goes." *Id.* at 505-506 (quoting *Ford*, 141 S. Ct. at 1026) (emphasis added). Instead, "the phrase 'relate to' incorporates real limits, as it must to adequately protect defendants foreign to a forum." (ECF 44 at 18 (quoting *Ford*, 141 S. Ct. at 1026).) At a minimum, "relatedness requires a close connection between contacts and injury." *Yamashita*, 62 F.4th at 506. If the defendant's "relevant conduct" (as opposed to "unconnected activities") does not establish purposeful direction, the requisite "connection

between the forum and the specific claims at issue" is "missing." *Bristol-Myers Squibb Co. v. Superior Court of Cal.*, 582 U.S. 255, 264-265 (2017) (citing *Walden*, 571 U.S. at 287).

Plaintiff's Amended Complaint still fails to establish that close connection between DarkMatter's challenged conduct and the United States. Plaintiff alleges that DarkMatter "market[ed] its cyber-security services to U.S. companies"; that the UAE previously contracted with a U.S. company to develop and use hacking technology, and that DarkMatter used the same technology and employees as that U.S. company; and that DarkMatter hired "U.S. individuals … who possessed unique cyber-hacking knowhow developed in the United States." (ECF 54 ¶¶ 7, 57-73, 110.) But this Court has already rejected similar allegations as insufficient. (ECF 44 at 19 (citing "the acquisition of exploits, reliance on U.S. technology and knowhow illegally transferred from CyberPoint, employment of U.S. individuals, and U.S. anonymization services").) Because only "contacts that the 'defendant *himself*' creates with the forum" count under the second prong, accepting such third-party contacts as sufficient would impermissibly "require th[e] Court to exercise personal jurisdiction over Defendants based solely on their knowledge of the third-party's contacts with the United States." (ECF 44 at 18 (quoting *Walden*, 571 U.S. at 284).)

Nor can Plaintiff show that any of her amended allegations include contacts "related to the conduct that ultimately underpins Plaintiff's claim, which is the allegedly tortious hack of Plaintiff's phone caused by malware." (ECF 44 at 19). To state a CFAA claim, Plaintiff must allege that Defendants "knowingly cause[d] the transmission of a *** code, *** and as a result of such conduct, intentionally *cause[d] damage without authorization, to a protected computer.*" 18 U.S.C. § 1030(a)(5)(A) (emphasis added). That conduct allegedly occurred in the UAE. (*See* ECF 54 ¶ 191 ("Defendants intentionally caused damage to parts of [Plaintiff's] iPhone by infecting it with an exploit and malware."); ECF 44 at 10-11 ("Defendants began their tort of knowingly

transmitting malware in a foreign country," and the malware allegedly "activated on the target's phone … outside of the forum.").) The "develop[ment] [of] expertise and knowhow in the forum that was later used to create the malware that [allegedly] infected Plaintiff's phone is not enough to confer jurisdiction," as those historical facts are far removed from the alleged tortious conduct. (ECF 44 at 19.) Similarly, "the technology that Defendants purchased from U.S.-based companies was altered in significant ways before being deployed in the hack of Plaintiff's phone." (*Id.*; *see* ECF 54 ¶ 93 (alleging Defendants "create[d]" and "upgrade[d]" technology platform).) More broadly, Plaintiff's causes of action simply are not closely connected to (and do not arise out of) Plaintiff's allegations about DarkMatter's general history, its corporate acquisitions, or its hiring and marketing practices—none of which could cause injuries like those Plaintiff alleges. *See Yamashita*, 62 F.4th at 505-506.

In short, none of DarkMatter's alleged conduct could lead it to "reasonably anticipate being haled into [U.S.] court" to answer for Plaintiff's claims. *Ford*, 141 S. Ct. at 1027. Plaintiff's reliance on DarkMatter's history and background would "collaps[e] the core distinction between general and specific personal jurisdiction." *Yamashita*, 62 F.4th at 506 (citation omitted). Indeed, if these sorts of allegations are sufficient, U.S. courts would become a universal forum to a broad range of "foreign-cubed" litigation—"where the plaintiffs are foreign, the defendants are foreign, and all the relevant conduct occurred abroad," *RJR Nabisco, Inc. v. European Cmty.*, 579 U.S. 325, 363 (2016) (Breyer, J., concurring in part and dissenting in part)—that could be deemed "related" in some fashion to a prior U.S. technology purchase, corporate transaction, or marketing / hiring decision. That is not the law.

3. Exercising Jurisdiction Over DarkMatter Would Be Unreasonable

Under the third prong, "[e]ven if Plaintiff had shown that Defendants had sufficient 'minimum contacts' with the United States … the exercise of jurisdiction over Defendants would be unreasonable." (ECF 44 at 20.) None of Plaintiff's new allegations alter that determination.

a. "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. "Great care and reserve should be exercised when extending our notions of personal jurisdiction into the international field." *Asahi Metal Indus. Co., Ltd. v. Superior Court of Cal.*, 480 U.S. 102, 115 (1987) (citation omitted); *see also Decker Coal Co. v. Commonwealth Edison Co.*, 805 F.2d 834, 841 (9th Cir. 1986) ("sovereignty interests may carry significant weight when jurisdiction is asserted over a defendant from a foreign country"). Thus, when applying these factors, "[t]he 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." (ECF 44 at 20 (quoting *Asahi*, 480 U.S. at 114)); *see also Asahi*, 480 U.S. at 115 (courts should not "find the serious burdens on an alien defendant outweighed by minimal interests on the part of the plaintiff or the forum").

b. All of the factors that this Court held made jurisdiction over DarkMatter "unreasonable" still weigh in DarkMatter's favor.

First factor. "[S]ending an iMessage from a foreign location, transmitted through U.S.-based servers, to a foreign phone with intent to hack the phone in the foreign locale[,] presents no

'purposeful interjection' in the United States' affairs." (ECF 44 at 20.) That is true regardless of whether that "nonresident" then unilaterally travels to the United States. *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)).

Third factor. An obvious conflict exists between jurisdiction here and the sovereignty of the UAE and Saudi Arabia, because Plaintiff's allegations concern events that occurred largely in those countries and directly implicate both governments. (*See* ECF 44 at 21 ("This court must consider both the 'procedural and substantive interests of other nations' in deciding whether to exercise jurisdiction." (quoting *Asahi*, 480 U.S. at 115))); *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). Specifically, the UAE's sovereignty cuts against Plaintiff given that the alleged "conduct relates to actions carried out at the direct behest of [that] foreign sovereign." (ECF 44 at 21.) The Amended Complaint implicates the sovereignty of Saudi Arabia as well, given Plaintiff's allegation of a "sham trial" arising from a Saudi "charging document" that allegedly "referenced [her] private communications." (ECF 54 ¶¶ 167, 169.)

Fourth factor. The United States continues to have no interest in adjudicating this "foreign cubed" dispute between a foreign plaintiff, foreign defendants, and foreign conduct. (*See* ECF 44 at 21 (finding this factor "weighs against the exercise of jurisdiction")); *Asahi*, 480 U.S. at 114 (forum's interest at least "considerably diminished" in a dispute between foreign parties). The United States certainly has no interest in potentially expanding personal jurisdiction to a vast number of foreign litigants who may wish to bring tort claims in U.S. courts based on historical or

otherwise attenuated U.S. contacts that, fairly considered, are "unrelated to the conduct that ultimately underpins [their] claim[s]." (ECF 44 at 19.)

Fifth factor. None of Plaintiff's amended allegations change the fact that resolving the controversy here would be inefficient because all relevant parties, documents, and witnesses are located abroad (likely in either the UAE or Saudi Arabia). (*See, e.g.*, ECF 44 at 22 (noting "the almost completely foreign nature of the tortious conduct at issue").)

c. Even with respect to the factors this Court found weighed in Plaintiff's favor, the amended allegations do not help.

Second factor. DarkMatter, a UAE company with no U.S. connections, "would face at least some burden" (ECF 44 at 20)—in fact, would be significantly burdened—if forced to defend 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."). Although this Court found that this factor favored Plaintiff because DarkMatter was "involved in other legal proceedings in the United States" (ECF 44 at 21), the prior lawsuit involving DarkMatter that Plaintiff cited (ECF 35 at 23) was dismissed *for lack of personal jurisdiction*. *See Oueiss v. Saud*, No. 1:20-cv-25022, 2022 WL 1311114, at *20-21 (S.D. Fla. Mar. 29, 2022).[3] That reinforces, rather than undermines, the "significant weight" this Court should give to "[t]he unique burdens" DarkMatter would face defending itself in this forum. *Asahi*, 480 U.S. at 114.[4]

[3] The plaintiff in *Oueiss* noticed an appeal of that dismissal, but voluntarily dismissed her appeal before briefing. *Oueiss v. Saud,* No. 22-11408-AA, 2022 WL 19692323 (11th Cir. Nov. 9, 2022).

[4] Any past proceedings against the individual Defendants, while insufficient to overcome the reasonableness factors, are irrelevant as to DarkMatter. *See, e.g.*, *Rush v. Savchuk*, 444 U.S. 320, 331-332 (1980) ("aggregating" defendants "in evaluating their ties to the forum" is "plainly unconstitutional").

Sixth factor. This Court previously found that Plaintiff had an "interest in her claims being adjudicated by a U.S. court" because the claims arose "under U.S. law." (ECF 44 at 22.) But Plaintiff fails to show that her claimed injury "cannot be effectively remedied" under another forum's laws. *Sinatra v. Nat'l Enquirer, Inc.*, 854 F.2d 1191, 1200 (9th Cir. 1988); *see also Hungerstation*, 857 F. App'x at 351, 352 (all factors "point[ed] in defendants' favor" even though plaintiff brought "several claims that arise under federal statutes"). Regardless, the Ninth Circuit "give[s] little weight" to the sixth factor. *Panavision Int'l, L.P. v. Toeppen*, 141 F.3d 1316, 1324 (9th Cir. 1998).

Seventh factor. This Court held that the seventh factor favored Plaintiff because her allegations, "if assumed to be true, would make the UAE a hostile forum." (ECF 44 at 22.) But "[t]he Plaintiff bears the burden of proving the unavailability of an alternative forum," *Core-Vent Corp. v. Nobel Indus. AB*, 11 F.3d 1482, 1490 (9th Cir. 1993), and Plaintiff has never addressed whether she could bring analogous claims in any number of other countries that might have more interest than the United States in adjudicating Plaintiff's claims.

Regardless, even if "the second, sixth, and seventh factors favor Plaintiff," that "is not sufficient to overcome the conclusion that the other reasonableness factors weigh against jurisdiction." (ECF 44 at 22-23.)

C. The Court Lacks Personal Jurisdiction Over The Individual Defendants[5]

The Amended Complaint largely assumes that the Court has jurisdiction over Adams, Baier, and Gericke based on the same allegations regarding DarkMatter's use of Apple servers to access Plaintiff's iPhone, DarkMatter's use of U.S. technology and knowhow, and Plaintiff's

[5] Contrary to the amended complaint, as indicated in the concurrently-filed declaration, Adams does not reside in the United States. (*See* Second Adams Decl. ¶ 8.) Accordingly, Rule 4(k)(2) applies to all individual Defendants.

unilateral travel to the United States. As discussed, those allegations are not enough. And because Adams, Baier, and Gericke are domiciled abroad (in the Middle East and Asia), substantially the same "reasonableness" analysis that applies to DarkMatter applies to them.

None of Plaintiff's new allegations overcome her more general failure to show that this Court has jurisdiction over the individual Defendants.

First, Plaintiff alleges for the first time that Baier specifically entered into contracts to acquire exploits from U.S. companies, and that each individual Defendant communicated with those companies "about how to configure [the exploits] into a hacking system." (ECF 54 ¶¶ 94, 96-97, 99, 102-103.) As discussed above, such allegations cannot establish express aiming, because the connections between the third-party companies and the United States is fortuitous. In any event, there are still no allegations that the individual Defendants played any role as to the specific tort alleged in this case.

Second, Plaintiff incorporates the DPA that the individual Defendants (but not DarkMatter) reached with the U.S. Department of Justice. (ECF 54 ¶ 3 & Ex. A.) But this Court already considered the DPA in its prior order dismissing the original complaint. (*See* ECF 44 at 4 n.3 (taking judicial notice of the DPA).) The DPA, moreover, contains only general allegations about the individual Defendants' roles at DarkMatter and broad participation in DarkMatter's activities; it does not mention Plaintiff or the harm that she allegedly suffered at all, or otherwise indicate the individual Defendants' participation in targeting any specific person. In any event, whether the facts in the DPA would support the federal government's *unchallenged* right to bring *criminal* proceedings against the individual Defendants has nothing to do with whether those facts support this Court's *disputed* personal jurisdiction over Defendants in this *civil* proceeding. When it comes

to criminal jurisdiction, "the law of personal jurisdiction is simply inapposite." *United States v. Ali*, 718 F.3d 929, 944 (D.C. Cir. 2013).

Third, Plaintiff incorporates consent agreements between the individual Defendants and the U.S. Department of State. (ECF 54 ¶ 175 & Ex. B.) Like the DPA, these agreements do not reference Plaintiff (explicitly or implicitly) and have no bearing on the Court's jurisdiction.

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

The Court may alternatively dismiss the Amended Complaint for failure to state a claim upon which relief can 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. Plaintiff's CFAA Claim (Count One) Should Be Dismissed

1. Plaintiff Seeks An Impermissibly Extraterritorial Application Of The CFAA

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). Because the CFAA does not reach wholly extraterritorial claims alleging foreign access to foreign devices resulting in foreign harm, Plaintiff's CFAA claims fail.

First, Plaintiff alleges that her phone qualifies as a "protected computer," 18 U.S.C. § 1030(a)(1), because it was "connect[ed] to the internet." (ECF 54 ¶ 182.) But under the statutory definition, a qualifying "protected computer … located outside the United States" must be "used in a manner that affects interstate or foreign commerce or communication *of the United States*." 18 U.S.C. § 1030(e)(2)(B) (emphasis added); *see RJR Nabisco*, 579 U.S. at 344 (foreign commerce does not "mean literally all commerce occurring abroad," but only commerce "directly involving

the United States"). Plaintiff does not plausibly allege any substantial nexus between her phone and the United States at the time of the hack. If a mere internet connection were enough, the CFAA would reach virtually any hack occurring anywhere in the world.

Second, although the CFAA reaches some foreign devices, it does not apply to foreign *conduct*, let alone wholly foreign claims. The presumption against extraterritoriality is a "presumption against application to *conduct* in the territory of another sovereign." *Kiobel v. Royal Dutch Petroleum Co.*, 569 U.S. 108, 119 (2013) (emphasis added). "[E]xclusively 'foreign conduct is generally the domain of foreign law.'" *Abitron Austria GmbH v. Hectronic Int'l, Inc.*, 600 U.S. ---, 2023 WL 4239255, at *3 (U.S. June 29, 2023) (quoting *Microsoft Corp. v. AT&T Corp.*, 550 U.S. 437, 455 (2007)). As the Supreme Court recently reaffirmed, applying the presumption requires first determining "whether 'Congress has affirmatively and unmistakably instructed that' the provision at issue should 'apply to foreign conduct.'" *Id.* at *4 (quoting *RJR Nabisco*, 579 U.S. at 335, 337). If not, courts determine "whether the suit seeks a (permissible) domestic or (impermissible) foreign application of the provision" by asking whether the "'*conduct relevant to [the provision's] focus* occurred in United States territory.'" *Id.* (quoting *WesternGeco LLC v. ION Geophysical Corp.*, 138 S. Ct. 2129, 2136 (2018)).

Here, the CFAA does not expressly apply to foreign conduct. The Supreme Court has "repeatedly held that even statutes … that expressly refer to '*foreign* commerce'… are not extraterritorial." *Abitron*, 2023 WL 4239255, at *5 (citations omitted). For the same reason, the statute's reference to certain *devices* located abroad does not necessitate application to foreign *conduct* (given that a domestic hack could target a device "located outside the United States"). Nor does the statute's application to "[w]hoever" commits a violation, because broad "generic terms like 'any' or 'every' do not rebut the presumption." *Id.* At a minimum, nothing in the statute

unmistakably expresses congressional intent to cover allegations concerning only foreign parties, devices, and injuries.

Plaintiff thus seeks an impermissible foreign application of the CFAA. The focus of the CFAA is "the unauthorized access of a protected computer." (ECF 54 ¶ 179). And all the alleged conduct relevant to that focus "took place outside the United States." *Kiobel*, 569 U.S. at 124. That is enough to dismiss Plaintiff's CFAA claim.

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

Alternatively, Plaintiff fails to state a CFAA claim because her allegations do not plausibly link any Defendant to the alleged unauthorized access.

The Amended Complaint describes 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, the individual Defendants' DPA and consent agreements with the State Department, 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 allegation connecting Defendants to the crucial factual basis for Plaintiff's CFAA claim: the alleged unauthorized access of her iPhone.

Only seven paragraphs of the Amended Complaint allege any connection between DarkMatter and Plaintiff's device, and those are either conclusory (ECF 54 ¶¶ 134, 224) or explicitly based on "information and belief," *i.e.*, speculative, and unsupported by specific facts connecting DarkMatter to the alleged hack (*id.* ¶¶ 135-139). Plaintiff's failure to plead specific, non-conclusory facts dooms her claims against DarkMatter. *See Iqbal*, 556 U.S. at 679.

The allegations about the individual Defendants are similarly deficient. The Amended Complaint alleges that Baier, Adams, and Gericke worked for a U.S.-based company in the UAE

called CyberPoint, later worked for DarkMatter, developed the companies' alleged hacking capabilities, directed their hacking operations, and had inauthentic Apple accounts. (ECF 54 ¶¶ 8-10, 62-70, 72-82, 87, 93-110, 131-132, 172-177, 218-224.) While the individual Defendants' alleged career paths and work for CyberPoint and DarkMatter are described in detail, only one paragraph alleges that they participated in hacking Plaintiff's iPhone. (*Id.* ¶ 224). It is wholly conclusory and thus insufficient to state a claim. *See Iqbal*, 556 U.S. at 679. The DPA and consent agreements do not help because, as noted, they do not mention Plaintiff at all. *See id.* 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)).

3. The CFAA Claim Fails To Meet The Statutory Requirements

Plaintiff's allegations also fail to satisfy any of the factors for a civil action under the CFAA. The CFAA authorizes a civil claim only if a person "suffers damage or loss by reason of a violation" involving one of five factors. 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 "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). These definitions "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 54 ¶¶ 184-185.) Neither is satisfied.

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

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).

The Amended Complaint's loss allegations merely track the statutory standard. (ECF 54 ¶¶ 203-205.) They do not support an inference that Plaintiff incurred $5,000 in costs. The Amended Complaint does not allege that Plaintiff paid the "cyber-security experts" she allegedly communicated with (*id*. ¶ 204), or that she made any expenditures at all. Nor does Plaintiff quantify the value of the time allegedly spent in response to the alleged hacks. (*Id.*)

None of the Amended Complaint's further allegations of loss meets the first statutory requirement, either. Plaintiff's alleged business, economic, and educational losses, which are not caused by interruption of service but instead by foreign governments' alleged misuse of information taken from her phone (ECF 54 ¶¶ 205-211), fall outside the limited parameters of the statutory definition of loss, which requires the "consequential damages [to be] incurred *because of interruption of service.*" 18 U.S.C. § 1030(e)(11) (emphasis added); *see 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 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) (same). Her alleged loss of a vehicle (ECF 54 ¶ 209) falls outside the CFAA's loss definition for the same reasons. *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 "this type of damage or loss is not recognized by the CFAA") (citing *Andrews*, 932 F.3d at 1263). Further, the alleged "impairment" to Plaintiff's "ability to carry out her human rights work" and "lost access to files" are not quantified (ECF 54 ¶¶ 205, 207), so do not satisfy the minimum value requirement. *See Brooks*, 2019 WL 2635594, at *24 (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).

Accordingly, this Court should dismiss the CFAA claim based on Plaintiff's insufficient "loss" allegations. *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 claim because alleged loss and damage not encompassed by CFAA definition); *Brooks*, 2019 WL 2635594, at *25 (dismissing claim for failure to allege loss under statutory definition); *Ramirez v. SupportBuddy Inc.*, No. 17-cv-5781, 2018 WL 2089362, at *4 (S.D.N.Y. May 4, 2018) (dismissing 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,

2011 WL 4343517, at *4 (S.D.N.Y. Aug. 17, 2011)); *Jensen v. Cablevision Sys. Corp.*, No. 17-cv-00100, 2017 WL 4325829, at *13 (E.D.N.Y. Sept. 27, 2017) (dismissing 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, 2012 WL 1997697, at *4 (W.D. Wash. June 1, 2012) (same).

b. The Amended Complaint Fails To Allege Facts Establishing Physical Injury

The statutory phrase "physical injury" encompasses injury that is "caused (or, in the case of an attempted offense, would, if completed, have [been] caused)" by the violation. 18 U.S.C. § 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 (citation omitted) (emphasis added); *see Andrews*, 932 F.3d at 1263 (CFAA does not cover "general injuries unrelated to the hacking itself"). 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).

Limiting damages this way also comports with congressional intent. Statutes that are "analogous" to common-law torts are generally subject to common-law "directness principles," including "some direct relation between the injury asserted and the injurious conduct alleged." *Bank of Am. Corp. v. City of Miami*, 581 U.S. 189, 201 (2017) (noting the "well established principle of [the common] law that in all cases of loss, [courts] are to attribute it to the proximate cause, and not to any remote cause" (first alteration in original)). A CFAA claim is akin to a common law tort action. *See* H.R. Rep. No. 98-894, at 20 (1984), *as reprinted in* 1984

U.S.C.C.A.N. 3689, 3706 ("The conduct prohibited is analogous to that of 'breaking and entering.'"). It is therefore subject to the "traditional requirement" of proximate cause, which asks "whether the harm alleged has a *sufficiently close connection to the conduct the statute prohibits*." *Bank of Am. Corp.*, 581 U.S. at 201 (emphasis added).

Section 1030(c)(4)(A)(i)(III)'s legislative history confirms Congress' intent to cover physical injuries directly resulting from disruption of computers and computer networks. As the Senate Report for the CFAA amendment adding "physical injury to any person" to the definition of "damage" explains, 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).[6] Section 1030(c)(4)(A)(i)(III) thus covers injury that flows directly from a violation. 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," S. Rep. No. 104-357, at 11—technological harms that directly cause physical injury.

By contrast, the term does not include physical injury resulting from misuse of information, which did not proximately result from the alleged technological harm. Plaintiff alleges her physical injury was caused by an independent, intervening cause—namely, the Saudi security

[6] Subsequent amendments moved the "physical injury to any person" factor and other statutory factors to § 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). That did not eliminate the requirement that a physical injury must be caused by a statutory offense. *See* 18 U.S.C. § 1030(c)(4)(A)(i)(III).

forces who allegedly harmed her. (ECF 54 ¶¶ 164-165, 171.) Such 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 also cannot proceed, for two reasons. *First*, because Plaintiff's standalone CFAA claim fails, the conspiracy claim does too. *See Andersen v. Atl. 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–Employers Health & Welfare Tr. Fund v. Philip Morris Inc.*, 185 F.3d 957, 969 (9th Cir. 1999)).

Second, the act of state doctrine precludes Plaintiff's CFAA conspiracy claim because the claim asks the Court to conclude that the UAE government's actions within its own territory are unlawful. The act of state doctrine "reflect[s] 'the strong sense of the Judicial Branch that its engagement in the task of passing on the validity of foreign acts of state may hinder' the conduct of foreign affairs." *W.S. Kirkpatrick & Co., Inc. v. Env'l Tectonics Corp.*, 493 U.S. 400, 404 (1990) (quoting *Banco Nacional de Cuba v. Sabbatino*, 376 U.S. 398, 423 (1964)). "In its modern formulation, the doctrine bars suit where '(1) there is an official act of a foreign sovereign performed within its own territory; and (2) the relief sought or the defense interposed [in the action would require] a court in the United States to declare invalid the [foreign sovereign's] official act.'" *Sea Breeze Salt, Inc. v. Mitsubishi Corp.*, 899 F.3d 1064, 1069 (9th Cir. 2018) (internal quotations omitted). In addition to these two "mandatory" factors, courts "also consider the extent to which 'the policies underlying' the doctrine 'justify its application'": (1) "the greater the degree of codification or consensus concerning a particular area of international law, the more appropriate it is for the judiciary to render decisions regarding it"; (2) "the less important the implications of

an issue are for our foreign relations, the weaker the justification for exclusivity in the political branches"; and (3) "[t]he balance of relevant considerations may also be shifted if the government which perpetuated the challenged act of state is no longer in existence." *Id.* at 1069, 1072-1073 (quoting *Sabbatino*, 376 U.S. at 428).

Both the mandatory factors and the principles underlying the doctrine direct the conclusion that it precludes the CFAA conspiracy claim. With regard to the former, the Amended Complaint alleges that Defendants participated in a conspiracy with "UAE officials" to violate the CFAA. (ECF No. 54 ¶¶ 216-225.) "[I]n the context of the act of state doctrine, [] an official's acts can be considered the acts of the foreign state[.]" *Samantar v. Yousuf*, 560 U.S. 305, 322 (2010); *accord Sea Breeze Salt*, 899 F.3d at 1069. Plaintiff uses "UAE officials" to mean officials of the UAE government; she alleges that the alleged hack "was part of the UAE's campaign of persecution against perceived dissidents of itself and Saudi Arabia." (ECF No. 54 ¶ 140; *see also id.* ¶¶ 65-86 (describing UAE's alleged use of hacking against human rights activists); *id.* ¶¶ 230-231 (alleging that UAE targeted Plaintiff and was aided and abetted by the individual Defendants and conspired with individual Defendants and DarkMatter "to persecute Ms. Alhathloul").) Plaintiff also alleges that the purported conspiracy occurred in the UAE. (*See id.* ¶¶ 55-86, 218-224.) Thus, for Plaintiff to prevail, this Court would have to conclude that the UAE government and Defendants agreed to act unlawfully in the UAE's territory.

The policies underlying the act of state doctrine also counsel in favor of its application here. As to the first factor, the CFAA is domestic, not international, law. The Amended Complaint does not allege that the CFAA's prohibitions are codified in international law or that there is otherwise any consensus regarding them. As to the second, the UAE is a close U.S. ally, which heightens the stakes for U.S. foreign relations. *See* Department of State, U.S. Relations With

United Arab Emirates, https://www.state.gov/u-s-relations-with-united-arab-emirates/. And as to the third, the fact that the UAE government remains in existence supports applying the doctrine.

Because the policy considerations underlying the act of state doctrine support its application, the claim should be dismissed. *See Sea Breeze Salt*, 899 F.3d at 1074, 1075 (affirming dismissal based on act of state doctrine); *see also Tiangang Sun v. China Petroleum & Chem. Corp. Ltd.*, No. 13-cv-05355, 2014 WL 11279466, at *3 & n.4, *9 (C.D. Cal. Apr. 15, 2014) (recognizing act of state doctrine as additional basis for dismissing claim that Chinese government officials and private actors conspired to attempt to arbitrarily arrest plaintiff).

C. Plaintiff's ATS Claim (Count Three) Should Be Dismissed

Plaintiff brings an ATS claim 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 54 ¶ 228.) 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*, 569 U.S. 108 (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 subject-matter 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." (citing *Kiobel*)). "[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. Moreover, an ATS plaintiff must plead domestic conduct that is "relevant to the statute's focus"; peripheral or incidental domestic conduct is not enough. *Doe I v. Cisco Systems, Inc.*, No. 15-16909, 2023 WL 4386005, at *8 (9th Cir. July 7, 2023) (quoting *Nestlé*, 141 S. Ct. at 1936); *see also, e.g.*, *Mastafa v. Chevron Corp.*, 770 F.3d 170, 185 (2d Cir. 2014) ("focus" of ATS is conduct that allegedly violates international law).

Plaintiff seeks an impermissible extraterritorial application of the ATS because she does not allege that any domestic conduct violated international law. Instead, Plaintiff was allegedly arrested in the UAE and harmed in the UAE and Saudi Arabia. (ECF 54 ¶¶ 20, 30-33, 156-164.) Moreover, all of the individual Defendants' conduct claimed to have aided and abetted the alleged persecution is alleged to have occurred in the UAE. Indeed, the Amended Complaint alleges no U.S.-related *conduct* other than fortuitous, peripheral, and incidental alleged contacts with U.S.-based servers (*id.* ¶¶ 111-117, 120-121) and Plaintiff's single, voluntary trip to the United States (*id.* ¶¶ 143-148). These allegations fall far outside of the territorial scope of the ATS and certainly are not of sufficient force to displace the presumption against extraterritoriality. *See, e.g.*, *Nestlé*, 141 S. Ct. at 1937 (dismissing ATS claims on extraterritoriality grounds where "nearly all the conduct" giving rise to the ATS claim occurred outside the United States).

Second, Plaintiff's ATS claim should be dismissed because Plaintiff does not allege a recognized tort on which an ATS claim may be based. Traditionally, ATS claims encompassed only three torts that were widely accepted under international law when the ATS was enacted: "violation of safe conducts, infringement of the rights of ambassadors, and piracy." *Sosa v. Alvarez–Machain*, 542 U.S. 692, 724 (2004). 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, 732 (citations omitted). "[A]ny claim based on the present-day law of nations [must] 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." *Id.* at 725. Efforts to expand this list are both generally disfavored and closely scrutinized. As courts 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*); *Moskovits v. Mercedes-Benz USA, LLC*, No. 1:21-CV-20122, 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 claim premised on violation of the Universal Declaration of Human Rights because plaintiff failed to allege that defendant "violated established international law").

Plaintiff seeks to bring her ATS claim based on the individual Defendants' alleged conspiracy to commit, or aid and abet, "persecution." (ECF 54 ¶¶ 230-231.) The Amended Complaint alleges that this persecution was a "widespread or systematic attack directed against 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.* ¶ 229.) 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 and during a brief visit to

the United States, and that UAE officials—not the individual Defendants—allegedly arrested and tortured her because of her human rights advocacy. (*Id.* ¶¶ 133-165.)

Plaintiff's conclusory allegations fail to connect any of the individual Defendants to the hacking Plaintiff alleges, as discussed. Regardless, Plaintiff cannot show a violation of "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 724-725. Her allegations of overseas assistance of a foreign sovereign's surveillance of non-U.S. persons do not constitute an actionable ATS claim. Accepting those allegations as sufficient would impermissibly 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*, 141 S. Ct. 2704 (2021).

In any event, Plaintiff's factual allegations—which concern only herself and three other individuals (ECF 54 ¶¶ 83, 85-86)—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 state claim for crimes against humanity). 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, Plaintiff's ATS claim would still fail.

CONCLUSION

For the foregoing reasons, the Amended Complaint should be dismissed with prejudice. *See Allen v. City of Beverly Hills*, 911 F.2d 367, 373 (9th Cir. 1990) ("futility of amendment" and a "previously amended … complaint" support denial of leave to amend).

Respectfully submitted,

Dated: July 10, 2023

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*)
James E. Tysse (*pro hac vice*)
jtysse@akingump.com
Caroline L. Wolverton (*pro hac vice)*
cwolverton@akingump.com
2001 K St., N.W.
Washington, D.C. 20006
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