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' REPLY IN SUPPORT OF MOTION TO DISMISS** **REQUEST FOR ORAL ARGUMENT**

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES:

STATUTES:

OTHER AUTHORITIES:

INTRODUCTION

Plaintiff's opposition to Defendants' motion to dismiss confirms that Plaintiff has not established personal jurisdiction over any Defendant. Her main argument is that Defendants engaged in tortious conduct *within* the forum. But no authority supports the novel idea that sending an iMessage from abroad to a phone located abroad constitutes conduct *within* the United States.

As for the purposeful direction analysis that applies to such extraterritorial conduct, Plaintiff's argument that she suffered the requisite harm in the United States—despite never setting foot there—fails the straight-face test. Plaintiff also maintains that sending an iMessage from overseas to a phone located overseas constitutes "express aiming" at the United States so long as the sender knows Apple's servers are located there. But Plaintiff did not even allege such knowledge. Regardless, the Supreme Court has made clear that knowledge of a third party's contacts with the forum cannot support personal jurisdiction. Plaintiff's expansive theory would lead to absurd results, as many foreigners engage in electronic messaging (and other activities) while aware that underlying technology uses servers located in the United States. Throughout her opposition, Plaintiff relies on cases involving defendants who directly stole or otherwise retrieved information from servers owned by plaintiffs, causing harm to those plaintiffs in the forum where the servers were located. But Plaintiff alleges nothing like that—she alleges that messages *passing through* third-party servers in the United States caused injury to her abroad. No court has exercised personal jurisdiction over a defendant based on such limited and fortuitous connections with the United States. And allegations that do not give rise to her claims (*e.g.*, about the general history of DarkMatter and the technology it uses) obviously do not support specific jurisdiction.

Nor, in any event, has Plaintiff stated a claim for relief under the Computer Fraud and Abuse Act (CFAA), or established this Court's subject matter jurisdiction under the Alien Tort Statute (ATS). As to the former, Plaintiff's arguments fail to overcome the deficiencies in the

Complaint that preclude her CFAA claim. Plaintiff's factual allegations do not support an inference that Defendants hacked her phone, or establish loss totaling at least $5,000 or physical injury caused by Defendants within the meaning of the CFAA. Nor can Plaintiff overcome application of the intra-corporate conspiracy doctrine, which bars her CFAA conspiracy claim. Her own allegations belie her argument that DarkMatter and the individual Defendants worked together in anything other than an employer-employee relationship. Plaintiff's ATS claim, asserted against only the individual Defendants, also fails: The weak U.S. connections she points to are insufficient to displace the presumption against extraterritoriality under binding precedent, and her allegations do not fit the narrow set of claims actionable under the ATS.

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

ARGUMENT

I. THE COURT LACKS PERSONAL JURISDICTION OVER ALL DEFENDANTS

Because Plaintiff does not dispute that Defendant Ryan Adams is domiciled abroad (*see* ECF 35, p. 12 & n.3), this Court's personal jurisdiction hinges on whether Plaintiff's allegations as to each Defendant satisfy Rule 4(k)(2) of the Federal Rules of Civil Procedure. (*See* ECF 28, p. 4.)[1] As to all Defendants, Plaintiff's allegations fall short. *First*, Plaintiff relies on the wrong legal standard by purporting to apply the general "purposeful availment" test, rather than the "purposeful direction" test that applies to claims involving alleged extraterritorial tortious conduct. *Second*, Plaintiff fails to show purposeful direction by (i) alleging no in-forum harm whatsoever and (ii) not showing express aiming, as the only link between her claims and the United States—the location of Apple's servers—is fortuitous. *Third*, contacts with the United States that are

[1] Citations to page numbers in court-filed documents refer to the internal pagination, not the ECF-pagination.

unrelated to this litigation cannot cure those failures. *Finally*, Plaintiff offers no persuasive reason why exercising jurisdiction over Defendants would be reasonable.

A. The Purposeful Direction Test, Not The Purposeful Availment Test, Governs Plaintiff's Extraterritorial Tort Allegations

Plaintiff argues that the general "purposeful availment" test applies to Defendants' alleged conduct. (ECF 35, pp. 13-14, 17-18.) Although "physical presence in the forum is not a prerequisite to jurisdiction," *Walden v. Fiore*, 571 U.S. 277, 285 (2014), the Ninth Circuit has made clear that a more specific test—the "purposeful direction" inquiry—controls whether tortious conduct outside the United States gives rise to personal jurisdiction. *See AMA Multimedia, LLC v. Wanat*, 970 F.3d 1201, 1208 (9th Cir. 2020). That inquiry is unnecessary for torts only if "committed within the forum." *Freestream Aircraft (Bermuda) Ltd. v. Aero Law Grp.*, 905 F.3d 597, 606 (9th Cir. 2018).[2]

Plaintiff attempts to bypass the purposeful direction inquiry by seeking application of the jurisdictional test that applies when tortious conduct occurs *within* the United States. (ECF 35, p. 13.) But Plaintiff's argument fails because she does not allege that Defendants took any "deliberate action within the forum[,]" *i.e.*, performed any of "the liability-producing acts *while physically present*" there. *Freestream*, 905 F.3d at 604, 606 (emphasis added) (quotation omitted). A party who engages in tortious conduct while physically present in the forum would typically have "voluntarily entered a [forum] and invoked the protection[] of [its] laws." *Id.* at 606 (third

[2] Plaintiff relies on the Ninth Circuit's statement that there is "no 'rigid dividing line'" between purposeful availment and purposeful direction. (ECF 35, pp. 17-18.) But the Court was referring to "[w]hen both contract and tort claims are at issue." *Global Commodities Trading Grp., Inc. v. Beneficio de Arroz Choloma, S.A.*, 972 F.3d 1101, 1107 (9th Cir. 2020). Plaintiff does not assert any contract claims. When only tort claims are at issue, courts determine the proper test by "taking into account where the allegedly tortious conduct occurred," and applying the "effects test" when the conduct occurred "outside the forum." *Freestream*, 905 F.3d at 605.

alteration in original) (quoting *Elkhart Eng'g Corp. v. Dornier Werke*, 343 F.2d 861, 868 (5th Cir. 1965)). By contrast, the "purposeful direction" test applies to persons, like Defendants, "who never physically entered the forum" while committing allegedly tortious acts. *Id.* at 604. A "purposeful direction analysis" including an "effects test" gauging the nexus between the alleged conduct and the forum simply "makes more sense when dealing with" such "out-of-forum tortfeasors." *Id*. at 605-606.

Attempting to shield her claims from that effects test, Plaintiff argues that "part of" Defendants' alleged tortious conduct occurred within the United States, because Defendants allegedly sent iMessages from abroad that were routed through Apple's servers in the United States on their way to Plaintiff's phone. (ECF 35, pp. 14-15.) But that would eliminate any distinction between (i) conduct within the forum and (ii) conduct that "takes place outside the forum" and purportedly "has effects inside the forum[.]" *AMA*, 970 F.3d at 1208 (emphasis omitted). It would also contradict the Ninth Circuit's recent decision in *Will Co., Ltd. v. Lee*, which applied the "purposeful direction" test to allegations that foreign defendants used a Utah-based server to host copyrighted content for a U.S. audience. Appeal No. 21-35617, Slip op. at 11 (9th Cir. Aug. 31, 2022) (attached as Appendix A).[3]

Plaintiff relies primarily on *Climax Portable Machine Tools, Inc. v. Trawema GmbH*, No. 3:18-cv-1825-AC, 2020 WL 1304487 (D. Or. Mar. 19, 2020), but the conduct in *Climax* bears no resemblance to the allegations here. *Climax* concerned the direct theft of trade secrets from a computer server owned by the plaintiff in Oregon. According to the court, that conduct constituted

[3] Plaintiff contends that "Defendants do not dispute that their malicious hack reached U.S. servers in order to infect Alhathloul's device." (ECF 35, p. 17.) But Defendants simply understand that Plaintiff's allegations must be taken as true on a motion to dismiss—and those allegations do not establish personal jurisdiction.

purposeful availment because the defendants "themselves retrieved items from that server for an unauthorized purpose," and even "reached out to . . . employees in Oregon to request confidential files and access to other confidential information in order to take trade secrets[.]" 2020 WL 1304487, at *6; *see also MacDermid, Inc. v. Deiter*, 702 F.3d 725, 730 (2d Cir. 2012) (retrieving confidential information from in-forum servers). In other words, the misappropriation of trade secrets had occurred in the forum because the trade secrets were physically in, and were stolen directly from, the forum.

By contrast, Plaintiff's claims arise from alleged unauthorized access to her phone and subsequent harms, all of which occurred in the Middle East. No element of the purported CFAA and ATS torts took place in the forum. Plaintiff cites no authority for the novel proposition that "knowingly caus[ing] the transmission" of code occurs not only where that code is sent from and to, but also wherever it travels along the way. (ECF 35, p.14.) And unlike stealing from a server in the forum, sending an iMessage merely involves a third party routing the message through its own server—with no access to the server's content (let alone theft) by any Defendant.

For the same reason, Plaintiff's laundry list of cases using purposeful availment language—many decided long before *Walden* emphasized that "random" and "fortuitous" contacts with "other persons affiliated with the [forum]" cannot support personal jurisdiction, 571 U.S. at 286—might be relevant if Apple had brought a lawsuit alleging harm to its servers in the United States, or if Plaintiff's iPhone had been located in the United States. But they do not come close to supporting Plaintiff's counterintuitive suggestion that sending an iMessage from abroad to an iPhone located

abroad constitutes "an intentional tort . . . committed within the" United States. *Freestream*, 905 F.3d at 606.[4]

In any event, *Climax*'s "purposeful availment" discussion is inconsistent with the Ninth Circuit's rule that the "effects test" applies to "out-of-forum tortfeasors," and that tortious conduct occurs within the forum only when the tortfeasor is "physically present" there. *Freestream*, 905 F.3d at 606. Applying that rule, the Ninth Circuit has recognized that, for personal jurisdiction purposes, remotely accessing a server occurs where the defendant, not the server, is located. *See Hungerstation LLC v. Fast Choice LLC*, 857 F. App'x 349, 351 (9th Cir. 2021) (where defendants "remotely access[ed] servers located in the United States," "the alleged tortious conduct took place in Saudi Arabia"); *see also Lee*, Appendix A, Slip op. at 11 (applying purposeful direction test for out-of-forum conduct to foreign defendants' alleged use of U.S. servers).

[4] Indeed, each is easily distinguishable as involving much more extensive in-forum conduct than having an electronic message traverse a U.S. server. *See Paccar Int'l, Inc. v. Commercial Bank of Kuwait, S.A.K.*, 757 F.2d 1058, 1064 (9th Cir. 1985) (defendant made "fraudulent demand for payment" in forum); *UMG Recordings, Inc. v. Kurbanov*, 963 F.3d 344, 354 (4th Cir. 2020) (defendant "registered . . . with the U.S. Copyright office," "contracted with U.S.-based advertising brokers," and directly "relied on U.S.-based servers"); *Wien Air Alaska, Inc. v. Brandt*, 195 F.3d 208, 213 (5th Cir. 1999) (defendant made fraudulent "misrepresentations" in "communications directed into [the] forum"); *HB Prods., Inc. v. Faizan*, Civ. No. 19-00487 JMS-KJM, 2022 WL 1523604, at *13-14 (D. Haw. May 13, 2022) (defendant hosted websites featuring pirated content on servers leased to him in the United States and "specifically chose servers with United States-based IP addresses so he could overcome blacklist restrictions that search engines often apply . . . and to increase service speed to users visiting his websites from the United States"); *Rhapsody Sols., LLC v. Cryogenic Vessel Alts., Inc.*, Civil Action No. H-12-1168, 2013 WL 820589, at *4 (S.D. Tex. Mar. 5, 2013) (defendant hired a third party to "install . . . software" at a company "whose server is located in [the forum]," and directly "log[ged] onto [the] server . . . in order to use [that] . . . software to view data"); *CoStar Realty Info., Inc. v. Meissner*, 604 F. Supp. 2d 757, 766 (D. Md. 2009) (defendant entered into license agreement with in-forum plaintiff and "repeatedly accessed" plaintiff's in-forum servers). Plaintiff also cites a case that squarely *undermines* her argument against applying the effects test. *Facebook, Inc. v. ConnectU LLC* did *not* hold that a tort was committed within the forum, but rather applied the "effects test" as a specific application of "the purposeful availment prong." No. C 07-01389 RS, 2007 WL 2326090, *5 (N.D. Cal. Aug. 13, 2007).

In sum, Plaintiff's cite no authority for applying the general purposeful availment test here. But even if Defendants (somehow) were deemed to have engaged in conduct within the forum because an iMessage they allegedly sent passed through an in-forum server, Plaintiff cites no authority for the proposition that such an insignificant connection to the forum could establish purposeful availment. As noted, this case is nothing like *Climax*, which involved the theft of trade secrets located *within the forum*.

B. Defendants Did Not Purposefully Direct Any Activities At The United States

Plaintiff argues in the "[a]lternative[]" that she can satisfy the "purposeful direction" test, which requires that Defendants (i) caused her harm that they knew would likely be suffered in the forum and (ii) expressly aimed their conduct at the forum. (ECF 35, p. 15); *see AMA*, 970 F.3d at 1208-1209. Plaintiff satisfies neither requirement.

1. Defendants Did Not Cause Harm That They Knew Would Likely Be Suffered In The United States

The lack of any alleged harm felt in the United States is fatal to Plaintiff's jurisdictional argument. (*See* ECF 28, pp. 9-10.) Plaintiff admits that the "'brunt of the harm' did not occur until [her] device was fully compromised," but contends that Defendants' alleged "harmful transmission" of malware through Apple's U.S. servers nonetheless "transformed Apple's secure messaging system into Defendants' personal malware delivery device." (ECF 35, p. 16.) Plaintiff does not allege there was any actual physical harm to Apple's servers, theft from the servers, or other specific harm in the United States. And Plaintiff cites no case recognizing her new "transform[ation]" theory of harm. Indeed, nothing supports Plaintiff's suggestion that a plaintiff may establish personal jurisdiction over a defendant by invoking harm to a third-party technology company. No such case exists, because *the plaintiff* must suffer "sufficient harm" in the forum "to warrant jurisdiction." *Dole Food Co. v. Watts*, 303 F.3d 1104, 1113 (9th Cir. 2002) (examining

whether plaintiff, "rather than its European subsidiaries," suffered harm in the forum). And here, Plaintiff has described no harm that she could have possibly "felt . . . within" the United States while she was thousands of miles away. *Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme*, 433 F.3d 1199, 1206 (9th Cir. 2006); *see also Brown v. Service Grp. of Am., Inc.*, No. 3:20-cv-2205-IM, 2022 WL 43880, at *3 (D. Or. Jan. 5, 2022) ("defendant's actions" must have been "performed for the very purpose of having their consequences felt in the forum"). The Court should dismiss Plaintiff's complaint on that straightforward basis alone.

2. Defendants' Alleged Conduct Was Not "Expressly Aimed" At The United States

In any event, Plaintiff's allegations do not satisfy the "express aiming" requirement, either. Plaintiff argues that "Defendants intentionally aimed their exploit and malware at Apple's U.S. servers to leverage vulnerabilities in Apple's iMessage system and reach [her] iPhone." (ECF 35, p. 15.) 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." *Lee*, Appendix A, Slip op. at 19 (emphasis omitted) (quoting *Hungerstation*, 857 F. App'x at 351). Because "the location of [a] server alone is insufficient to establish personal jurisdiction," even intentionally "choosing to host [a website] in Utah" does not automatically qualify as express aiming at the United States. *Id.* at 17, 19 (emphasis omitted); *see id.* at 12 (basing jurisdiction not merely on defendants' undisputed choice to host content on U.S. server, but on additional evidence that defendants "both actively appealed to and profited from an audience in th[e]" United States) (quotations and alterations omitted). Here, there is no such targeting of the forum, and the happenstance that Apple unilaterally routes its iMessages through U.S. servers is insufficient to establish personal jurisdiction.

Plaintiff attempts to distinguish *Hungerstation* on the ground that there, the defendants' "access" of an in-forum server occurred via "a computer terminal located abroad." (ECF 35, p. 19.) But here, Defendants did not "access" any in-forum server *at all*. For all of Plaintiff's heated rhetoric characterizing sending an iMessage as a "sophisticated attack[] on U.S. Servers," (*id.* at 20), Plaintiff does not allege that Defendants communicated with anyone in the United States, accessed information on any servers in the United States, or took anything from such servers. Instead, Plaintiff alleges that Defendants sent an iMessage, triggering an automated process that (apparently) involves U.S.-based servers. Defendants' alleged claim-specific connections to the United States are thus even weaker than the insufficient contacts at issue in *Hungerstation*.

For the same reason, Plaintiff's argument that courts "have found express aiming where a defendant uses an in-forum server to commit a tort" (ECF 35, pp. 15-16), relies on a host of inapposite cases involving intentional targeting of in-forum servers or residents. *See supra* n.3; *DEX Sys., Inc. v. Deutsche Post AG*, 727 F. App'x 276, 278 (9th Cir. 2018) (defendant directly used, interacted with, and received data from a server that, "pursuant to an agreement reached by the parties," was located in the forum); *Felland v. Clifton*, 682 F.3d 665, 676 n.3 (7th Cir. 2012) (defendant "purposefully sent . . . emails to [forum] residents knowing that they would most likely be read and have their effect in [the forum]"); *NetApp, Inc. v. Nimble Storage, Inc.*, 41 F. Supp. 3d 816, 826 (N.D. Cal. 2014) (defendant improperly accessed Plaintiff's password-protected computer systems located in the forum); *Vivint, Inc. v. Bailie*, No. 2:15-CV-685-DAK, 2017 WL 396655, at *3 (D. Utah Jan. 30, 2017) (same). These authorities undermine, rather than support, Plaintiff's argument that sending an iMessage anywhere in the world is equivalent to "us[ing]" a server in the United States. Plus, many courts—including the Ninth Circuit in *Hungerstation*—have held that using an in-forum server does *not* give rise to jurisdiction when the alleged conduct

giving rise to a plaintiff's claims would be the same regardless of where the server was located. 857 F. App'x at 351; *see also Future World Elecs., LLC v. Results HQ, LLC*, No. CV 17-17982, 2018 WL 2416682, at *3 (E.D. La. May 29, 2018) (location of server "fortuitous" when it lacks "any bearing on defendants' conduct"). (ECF 28, pp. 6-7 & n.1 (collecting cases).)

Straining to strengthen the connection between her claims and the forum, Plaintiff argues that Defendants must have known that Apple's servers were located in the United States. (ECF 35, pp. 18-20.) But unlike in *Climax*, Plaintiff never even alleges such knowledge in the complaint. Moreover, simple knowledge that a message will be sent via Apple's servers is not equivalent to knowledge that it will be sent via Apple's *U.S.* servers. Yet even if Plaintiff adequately alleged knowledge, so what? The Supreme Court has "consistently rejected attempts to satisfy the defendant-focused 'minimum contacts' inquiry by demonstrating contacts between . . . third parties . . . and the forum[.]" *Walden*, 571 U.S. at 284. The whole point of *Walden* was that a defendant's "knowledge" of a fortuitous connection to the forum makes it no less fortuitous. *Id.* at 289. In *Walden*, a Nevada district court lacked personal jurisdiction even though the defendant "*knew* his allegedly tortious conduct in Georgia would delay the return of funds to plaintiffs with connections to Nevada." *Id.* at 279 (emphasis added). That is because focusing on a defendant's "knowledge" of a plaintiff's or third party's connections to the forum "improperly attributes" those connections "to the defendant," particularly when "none of [the] challenged conduct ha[s] anything to do with [the forum] itself." *Id.* at 289. Here, as in *Walden*, "no part of [Defendants'] course of conduct occurred in [the forum]," and Defendants "never traveled to, conducted activities within, contacted anyone in, or sent anything or anyone to [the forum]." *Id.* at 288-289. Plaintiff purports to rely on decisions where courts mentioned Defendants' knowledge of where a server was located, but each (again) involves more direct targeting of the technology in the forum. *See Oregon Int'l*

Airfreight Co. v. Bassano, No. 3:21-cv-01480-SB, 2022 WL 2068755, at *3-5 (D. Or. May 16, 2022), *report and recommendation adopted*, No. 3:21-cv-01480-SB, 2022 WL 2066188 (D. Or. June 8, 2022) (relying exclusively on analogy to *Climax*); *WhatsApp Inc. v. NSO Grp. Technologies Ltd.*, 472 F. Supp. 3d 649, 671-673 (N.D. Cal. 2020) (holding it was "critical" that (i) servers were owned by the plaintiff, "not . . . third parties," and (ii) "defendants' program sought out specific servers," such that the "location of the servers" was "central to the alleged tortious conduct").

Plaintiff also attempts to gin up express aiming based on a deferred prosecution agreement (DPA) that the individual Defendants (but not DarkMatter) reached with the U.S. Department of Justice. (ECF 35, pp. 18-19.) Even putting aside that Plaintiff omitted most of those allegations from her complaint, whether those facts would support the federal government's *unchallenged* right to bring *criminal* proceedings against the individual Defendants has nothing to do with whether they 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). Indeed, while courts routinely dismiss civil cases based on due process principles due to insufficient links between the extraterritorial allegations and the United States, *see, e.g.*, *AMA*, 970 F.3d at 1212; *Asahi Metal Indus. Co. v. Superior Ct. of Cal., Solano Cnty.*, 480 U.S. 102, 116 (1987), in *Ali* the D.C. Circuit stated that it had "not found . . . any case in which extraterritorial application of a federal criminal statute was actually deemed a due process violation." 718 F.3d at 944 n.7. Further, this part of

Plaintiff's argument relies on the DPA only to establish Defendants' knowledge that Apple servers were located in the United States. As explained, such knowledge does not move the needle.[5]

Nor can Plaintiff defend the absurd results that would flow from her express aiming theory. As Defendants have explained (ECF 28, p.8), that theory would result in near-universal jurisdiction over claims involving communications between wholly foreign parties, at least so long as those parties were—in Plaintiff's words—"sophisticated" enough to know that they are using technology that relies on servers in the United States. (ECF 35, p. 19.) For example, under Plaintiff's theory, a foreign person sophisticated enough to know that Google has servers in California could be haled into this forum after sending a tortious email to a foreign recipient with a "gmail.com" address.

The logic of Plaintiff's theory would also extend beyond communications technology. For example, it would support a Tennessee court exercising jurisdiction over a person who mails a product from Oregon to Virginia, so long as the sender happened to know that the shipping company would route the product through a distribution center in Tennessee. But that would allow jurisdiction to turn on facts that are irrelevant to the Supreme Court's test, which focuses on the "relationship among the defendant, the forum, and the litigation." *Walden*, 571 U.S. at 284 (quoting *Keeton v. Hustler Mag., Inc.*, 465 U.S. 770, 775 (1984)).

[5] Plaintiff's opposition does not purport to separately analyze the individual Defendants' litigation-related connections with the United States, which are even weaker than DarkMatter's because Plaintiff does not allege any specifics about the individual Defendants' purported roles in the alleged scheme. (*See* ECF 28, p. 13.) Plaintiff's belated reliance on the DPA does not cure that failure, because the DPA contains only general allegations about the individual Defendants' roles at DarkMatter and broad participation in DarkMatter's activities, and does not mention Plaintiff or the harm she allegedly suffered. Plaintiff attempts to brush that aside (ECF 35, p. 26, n.8), but the point is that Plaintiff's attempt to attribute jurisdictional significance to the DPA as to Plaintiff's specific claims founders on (among other things) the DPA's wholly *unspecific* narrative.

C. Plaintiff's Claims Do Not Arise Out Of Or Relate To Defendants' Alleged United States Contacts

Because Defendants' alleged "contact" with Apple's servers is jurisdictionally insignificant, Plaintiff cannot demonstrate the minimum contacts to the United States to demonstrate personal jurisdiction. The Court should reject Plaintiff's attempt to manufacture personal jurisdiction based on alleged contacts from which her claims do not arise. Jurisdiction requires "[an] activity or an occurrence that takes place in the forum . . . and is therefore subject to [its] regulation." *Ford Motor Co. v. Montana Eighth Jud. Dist. Ct.*, 141 S. Ct. 1017, 1025 (2021). "For this reason, 'specific jurisdiction is confined to adjudication of issues deriving from, or connected with, the very controversy that establishes jurisdiction." *Bristol-Myers Squibb Co. v. Superior Ct. of Cal., S.F. Cnty.*, 137 S. Ct. 1773, 1780 (2017) (quoting *Goodyear Dunlop Tires Operations, S.A. v. Brown*, 564 U.S. 915, 919 (2011)). Jurisdiction over an alleged "intentional tortfeasor must be based on intentional conduct by the defendant that creates the necessary contacts with the forum." *AMA*, 970 F.3d at 1209 n.5 (quoting *Walden*, 571 U.S. at 286). If the defendant's "relevant conduct" (as opposed to the defendant's "unconnected activities") does not establish purposeful direction, the requisite "connection between the forum and the specific claims at issue" is "missing." *Bristol-Myers Squibb*, 137 S. Ct. at 1781 (citing *Walden*, 571 U.S. at 287). Thus, what matters is the relationship between a defendant's "challenged conduct" and the forum. *Walden*, 571 U.S. at 289.

Here, Plaintiff's motley collection of U.S.-based contacts has nothing to do with the torts she alleges. Plaintiff appears to understand that Defendants' general history is irrelevant to this Court's jurisdiction, and does not rely on it in the bulk of her argument. But when confronted with (i) *Hungerstation*'s rejection of Plaintiff's server theory and (ii) the requirement that this suit arise out of or relate to Defendants' forum-related activities, Plaintiff pivots to relying on Defendants'

alleged "acquisition of exploits, reliance on U.S. technology and knowhow . . ., employment of U.S. individuals, and U.S. anonymization services." (ECF 35, pp. 20, 22.) None of that is Defendants' allegedly tortious conduct. The allegedly tortious conduct was "sending an exploit and malware to the phone through Apple's U.S.-based servers." (ECF 1, ¶¶ 141; *see also id.* ¶¶ 140-152.) Nor do Plaintiff's claims involve allegations that Defendants "exploited [a] market," "enter[ed] a contractual relationship," did "substantial business," or "actively [sought] to serve" anyone in the forum, or any other "activity or . . . occurrence" by which Defendants' litigation-related efforts "deliberately extended into" the forum. *Ford*, 141 S. Ct. at 1025-1027. In short, "the forum . . . and the defendant[s'] activities there, lack[] any connection to [Plaintiff's] claims." *Id.* at 1031.

D. Exercising Personal Jurisdiction Over Defendants Would Be Unreasonable

Even if Plaintiff showed that Defendants had the required minimum contacts with the United States, she has not showed that exercising jurisdiction over Defendants would be reasonable.

First, Plaintiff's argument that Defendants "purposefully interjected themselves into" the United States merely restates her (flawed) premise that Defendants engaged in "tortious activity inside the forum." (ECF 35, p. 23.) Second, Plaintiff argues that Defendants "raise only a minimal burden" because they are "currently involved in other legal proceedings in the United States," citing the DPA in particular. (*Id.*) This argument cannot support jurisdiction over DarkMatter, which is not a party to the DPA. And, as to the individual Defendants, Plaintiff's contention ignores the obvious burdens that litigating in the United States imposes on any nonresident—and that the whole point of agreeing to a DPA is to *avoid* further burdensome proceedings. Third, Plaintiff concedes that her allegations "relate to conduct" purportedly "carried out at the behest of the UAE government," yet inexplicably professes ignorance as to how this case would implicate

the UAE's interests. (*Id.*, at 24.) Fourth, Plaintiff contends that the United States has an interest in regulating "violations of U.S. law," again citing the DPA—but fails to acknowledge that the United States' interest is "considerably diminished" when the purported "violations" involve extraterritorial conduct and parties. (*Id.*); *see, e.g.*, *Asahi*, 480 U.S. at 115. Plaintiff attempts to make much of the DPA's clarification that it "does not provide any protection for any . . . civil matter" (ECF 35, Ex. A, p. 9 ¶ 24), but that statement only reinforces that a deferred prosecution agreement has nothing to do with civil litigation, let alone civil personal jurisdiction. Fifth, Plaintiff attempts to downplay how inefficient proceedings in the District of Oregon would be for all involved, but cannot ignore that the core parties, documents, and witnesses are located abroad. (ECF 35, p. 25.) All Plaintiff can muster is that "Apple's technology experts and the companies that designed and sold the exploits [allegedly] used by Defendants" are located in the United States. *Id.* But they are not located *in Oregon*, and such potential witnesses would play (at most) a peripheral role in this dispute. Sixth, Plaintiff raises no separate basis for why this forum—compared to any other in the world—is most likely to provide convenient and effective relief. (*Id.*) Seventh, when the preceding factors demonstrate that a plaintiff's chosen forum is "unreasonable," the plaintiff has the "burden to show that another forum is unavailable." *Sinatra v. National Enquirer, Inc.*, 854 F.2d 1191, 1201 (9th Cir. 1988). But Plaintiff does not meaningfully attempt to establish the unavailability of an alternative forum. She protests (without authority or evidence) that the UAE is not "viable," but never addresses the possibility that she could bring identical or analogous claims in other places not governed by the U.S. Constitution's due process protections for civil defendants.

"Great care and reserve should be exercised when extending our notions of personal jurisdiction into the international field." *Asahi*, 480 U.S. at 115 (quotation omitted). In light of

the relevant factors, there is "a compelling case that the exercise of jurisdiction would not be reasonable." *Shwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 802 (9th Cir. 2004).

*****

For all these reasons, the Court lacks personal jurisdiction over Defendants.

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

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

1. *Neither The DPA Nor The Reuters Article Suffices To Support The CFAA Claim*

Faced with dismissal of her CFAA claim due to a lack of factual allegations plausibly linking any of the individual Defendants or DarkMatter to the alleged hacking of Plaintiff's iPhone , Plaintiff relies largely on the DPA. But an attachment to an opposition brief is not part of the Complaint and cannot supply allegations not stated in the Complaint. *Schneider v. California Dep't of Corr.*, 151 F.3d 1194, 1197 n.1 (9th Cir. 1998) ("In determining the propriety of a Rule 12(b)(6) dismissal, a court *may not* look beyond the complaint to a plaintiff's moving papers, such as a memorandum in opposition to a defendant's motion to dismiss."). Regardless, the DPA (as noted above) makes no mention of Plaintiff, and her suggestion that it implicitly supports her allegations is mere speculation.

Similarly, the only allegation in the Complaint tying Defendants to Plaintiff is a single paragraph incorporating a *Reuters* article about DarkMatter. (ECF 1 ¶ 107.) As Defendants explained, that conclusory allegation is not enough. (ECF 28, p. 15.) While "information and belief" allegations may be permissible where facts are peculiarly in a defendant's possession, they must be accompanied by "sufficient data to justify interposing an allegation on the subject." *Covelli v. Avamere Home Health Care LLC*, No. 3:19-CV-486-JR, 2021 WL 1147144, at *4 (D. Or. Mar. 25, 2021) (Simon, J.) (quoting 5 CHARLES A. WRIGHT, ARTHUR R. MILLER & A.

BENJAMIN SPENCER, FED. PRAC. & PROC. CIV. § 1224 (4th ed. 2022)). Here, the Complaint provides no specific facts connecting Defendants to the alleged hack of Plaintiff's phone.

2. Plaintiff Has Failed To Show That The CFAA Allegations Meet The Statutory Requirements

Plaintiff's CFAA claim also fails because the Complaint does not allege a loss or physical injury connected to the alleged hacking within the meaning of the statute.

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

Plaintiff does not dispute that "loss" under the CFAA focuses on technological harms and consequential damages that result from interrupted service. *See Van Buren v. United States*, 141 S. Ct. 1648, 1660 (2021); 18 U.S.C. § 1030(e)(11). Yet her alleged harms fall far outside the "narrow" and "limited parameters" of the term as used in the CFAA. *Andrews v. Sirius XM Radio, Inc.*, 932 F.3d 1253, 1262-1263 (9th Cir. 2019).

For starters, Plaintiff's allegations of technological harm are unsupported by any factual detail. (ECF 1 ¶ 154 (alleging "costs incurred due to responding to the hack, conducting a damage assessment, and attempting to restore data").) Consequently, they fail to satisfy the statutory requirement of at least $5,000 in loss or damages. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) ("Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice.") (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007)).

In contrast, the cases on which Plaintiff relies involved more specific allegations of loss. *See Cantu v. Guerra*, No. SA-20-CV-0746-JKP-HJB, 2021 WL 2652933, at *5 (W.D. Tex. June 28, 2021) (although plaintiff's allegations in some respects "merely parrot" the statutory definition of loss, they also specified that she had engaged a digital forensics company); *Freedom Banc Mortg. Servs., Inc. v. O'Harra*, No. 2:11-CV-01073, 2012 WL 3862209, at *7 (S.D. Ohio Sept. 5, 2012) (plaintiff alleged lost revenue from failure of computers due to the defendants' conduct).

Plaintiff's claimed consequential damages also fall outside the statutory definition of loss because the Complaint does not allege any facts tying the claimed losses to interruption of service on Plaintiff's phone, which she acknowledges is a statutory requirement. (*See* ECF 35, p. 33.) What Plaintiff claims as consequential damages—lost access to files on her phone, a cancelled business contract, impoundment of a vehicle, and disruption of Plaintiff's life, schooling, and career (*see* ECF 1 ¶¶ 156-160)—result from the alleged misuse of information taken from her phone, not interruption of service on the phone. Specifically, Plaintiff's allegations indicate that her consequential damages (including loss of access to files on her phone) resulted from her alleged arrest and detention by officials of foreign governments. (ECF 1 ¶¶ 124-125, 130.) Again, those alleged losses result not from interruption of service, but from *use* of unlawfully accessed information, which falls beyond the CFAA. *Fraser v. Mint Mobile, LLC*, No. C 22-00138 WHA, 2022 WL 1240864, at *5 (N.D. Cal. Apr. 27, 2022); *see also Wofse v. Horn*, 523 F. Supp. 3d 122, 139 (D. Mass. 2021) (lost business income, which did not result from interruption of service, did not qualify as loss under the CFAA). Further, Plaintiff's alleged lost access to files on her phone is not quantified, such that it cannot satisfy the statutory $5,000 minimum requirement. *See Brooks v. Agate Res., Inc.*, No. 6:15-CV-000983-MK, 2019 WL 2635594, at *24 (D. Or. Mar. 25, 2019), *report and recommendation adopted*, No. 6:15-CV-000983-MK, 2019 WL 2156955 (D. Or. May 14, 2019), *aff'd*, 836 F. App'x 471 (9th Cir. 2020) (holding that CFAA plaintiff failed to allege minimum required loss where he "fail[ed] to quantify [his alleged] damages").

Plaintiff now suggests that "interrupted critical security services" undermined her human rights work, but that argument is not grounded in any factual allegations in the Complaint. (*See* ECF 35, p. 33.) Plaintiff cites allegations that describe only impairment of the phone's security features and say nothing about any impact on her work. (*See id.* (citing ECF 1 ¶¶ 101, 152-153).)

In any event, the Plaintiff does not quantify any impact on her work, so there is no basis for inferring a loss greater than the statutory $5,000 minimum. *Brooks*, 2019 WL 2635594, at *24.

b. Physical Injury From Third-Party Use Of Accessed Information Does Not Support A Claim Under The CFAA

While physical injury is distinct from "loss" under the CFAA, physical injury must be "caused" by prohibited conduct to support a civil action. 18 U.S.C. § 1030(c)(4)(A)(i)(III) ("the offense caused (or, in the case of an attempted offense, would, if completed, have caused) … physical injury to any person"). Plaintiff's reliance on physical injury caused by third parties using information obtained through prohibited conduct to support a civil claim under the CFAA runs afoul of 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." *Bank of Am. Corp. v. City of Miami*, 137 S. Ct. 1296, 1305 (2017) (alteration omitted). Like the Fair Housing Act ("FHA") claim in *Bank of America*, a CFAA claim is akin to a tort action, *see* H.R. REP. NO. 98-894, at 20 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3706 ("The conduct prohibited is analogous to that of 'breaking and entering.'"), and therefore subject to the "traditional requirement" of proximate cause. *Bank of Am. Corp.*, 137 S. Ct. at 1305.

For federal statutory claims, "[p]roximate-cause analysis is controlled by the nature of the statutory cause of action. The question it presents is whether the harm alleged has a *sufficiently close connection to the conduct the statute prohibits*." *Bank of Am. Corp.*, 137 S. Ct. at 1305 (emphasis added). The cases recognizing the requirement of a close connection between a CFAA violation and alleged loss to state a claim under 18 U.S.C. § 1030(c)(4)(A)(i) are therefore useful in considering the sufficiency of the connection between the alleged CFAA violation and Plaintiff's claimed physical injury vis-à-vis section 1030(c)(4)(A)(i)(III). *See Van Buren*, 141 S. Ct. at 1660; *Andrews*, 932 F.3d at 1263; *Fraser*, 2022 WL 1240864, at *5. The physical injury Plaintiff

alleges—detention and torture by foreign government officials—lacks a close connection to the computer hacking conduct by private actors that the CFAA prohibits. *See Van Buren*, 141 S. Ct. at 1660 (recognizing that the CFAA is "aimed at preventing the typical consequences of hacking" (quoting *Royal Truck & Trailer Sales & Serv., Inc. v. Kraft*, 974 F.3d 756, 760 (6th Cir. 2020))); *see also United States v. Nosal*, 676 F.3d 854, 857 (9th Cir. 2012) (en banc) (describing CFAA as "an anti-hacking statute"). It is therefore insufficient to state a claim under section 1030(c)(4)(A)(i)(III). *See Van Buren*, 141 S. Ct. at 1660; *Andrews*, 932 F.3d at 1263; *Fraser*, 2022 WL 1240864, at *5.

In an analogous context, the Supreme Court has rejected the foreseeability argument that Plaintiff advances. Plaintiff argues that UAE officials' alleged use of hacked information to harm Plaintiff was foreseeable. (ECF 35, p. 29.) But *Bank of America* held that "foreseeability alone does not ensure the close connection that proximate cause requires." 137 S. Ct. at 1306. In that case, nothing in the FHA suggested congressional intent to provide a remedy for the "ripples of harm" that flow from an FHA violation even if they were foreseeable. *Id.* Similarly, nothing in the CFAA suggests that Congress intended to provide a remedy for harm rippling beyond the immediate effects of a CFAA violation. Like the Supreme Court recognized in *Bank of America* in the context of the FHA, "entertaining suits to recover damages for any foreseeable result of an [CFAA] violation would risk massive and complex damages litigation." *Id.* (internal quotation marks and citation omitted). Plaintiff's reliance on contrary California state law is therefore unavailing in determining proximate cause under the CFAA.[6]

[6] Both cases that Plaintiff cites in support of her foreseeability argument apply California law. (*See* ECF 35, p. 29.) *Ileto v. Glock Inc.*, 349 F.3d 1191, 1208 (9th Cir. 2003) ("*[U]nder California law*, where an intervening act by a third party was foreseeable, it does not amount to a superseding cause relieving the negligent defendant of liability." (emphasis added)); *Fraser*, 2022 WL 1240864 at*2-3 ("*Under California law*: 'The defense of superseding cause absolves the original tortfeasor,

The two CFAA cases on which Plaintiff relies for her physical injury argument support interpreting section 1030(c)(4)(A)(i)(III) to require a direct connection between a statutory violation and alleged physical injury, and to exclude injury caused by a third-party's alleged use of information obtained through a violation. (ECF 35, p. 31.) In *Wofse v. Horn*, the alleged physical injury (anxiety and related emotional harms) directly stemmed from "a prolonged series of multifaceted cyberattacks," rather than a third party's use of information procured through a CFAA violation. 523 F. Supp. 3d at 137 ("[T]here is evidence that 'as a result of the attacks,' [the plaintiff] began to suffer from anxiety, panic attacks, insomnia, and internal bleeding," and "[o]n this basis, a reasonable jury could conclude that the [defendants'] cyberattacks caused [the plaintiff] to suffer a physical injury[.]" (quoting physician letter)). And *Fraser* declined to extend the CFAA's civil cause of action to loss that flowed from a third party's misuse of unlawfully obtained information—despite separately finding that the misuse was sufficiently foreseeable to establish proximate cause *under California law*. 2022 WL 1240864 at *5 (theft of cryptocurrency which flowed from a third party's use of the unlawfully obtained information was "not recognized by the CFAA"). Plaintiff identifies no reason why the CFAA's civil cause of action would exclude financial loss flowing from third-party use of unlawfully obtained information, as *Fraser* held, but would encompass physical injury flowing from such third-party use.

The Senate Report's explanation that Congress added "physical injury" to the Act to address its concern about computer intrusions "causing physical injury to any person" confirms that section 1030(c)(4)(A)(i)(III) covers injury that flows directly from a violation rather than from

---

even though his conduct *was* a substantial contributing factor, when an independent event subsequently intervenes in the chain of causation, producing harm of a kind and degree so far beyond the risk the original tortfeasor should have foreseen that the law deems it unfair to hold him responsible.'" (emphasis added) (quoting *Chanda v. Federal Home Loans Corp.*, 215 Cal. App. 4th 746, 755 (2013))).

a third party's use of unlawfully obtained information. S. REP. NO. 104-357, at 11 (1996). That the Report relates to an earlier version of the statute, which included the term in the definition of "damage" (as Defendants' motion noted, *see* ECF 28, p. 20), does not lessen its import. The amendment moving the physical injury provision to its own subsection did not eliminate the requirement that, to be encompassed by the Act, a physical injury must be caused by a statutory offense. The current CFAA retains the requirement that, like the other statutory factors that can support a civil action, physical injury must be "caused (or, in the case of an attempted offense, would, if completed, have [been] caused)" by the offense. 18 U.S.C. § 1030(c)(4)(A)(i)(III).

Plaintiff attempts to broaden the CFAA's loss definition by relying on the statute's statement that a civil action is available if the conduct "involves" one of the enumerated statutory factors. (ECF 35, p. 32 (citing 18 U.S.C. § 1030(g)).) But that statement should be interpreted consistent with the statutory requirement of causation, 18 U.S.C. § 1030(c)(4)(A)(i)(III), and the proximate-cause requirement of a close connection between the alleged conduct the CFAA prohibits and the alleged harm, *Bank of Am.*, 137 S. Ct. at 1305. Indeed, the plain meaning of "involve" supports interpreting it to require a close connection between a violation and alleged harm. MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 616 (10th ed. 2000) ("2. a: to have within or as part of itself: INCLUDE[,] b: to require as a necessary accompaniment: ENTAIL") (*also available at* https://www.merriam-webster.com/dictionary/involve (last visited Sep. 8, 2022)).

*****

Because Plaintiff does not allege "loss" of at least $5,000 or physical injury within the meaning of section 1030(c)(4)(A)(i)(III), her CFAA claim should be dismissed.

B. Plaintiff Cannot Avoid Dismissal Of Her Conspiracy Claim (Count Two) Under The Intra-Corporate Conspiracy Doctrine

As Plaintiff's cited case recognizes, "as a matter of law agents or employees cannot conspire with their principal or employer." *McGraw Co. v. Aegis Gen. Ins. Agency, Inc.*, No. 16-CV-00274-LB, 2016 WL 3745063, at *7 (N.D. Cal. July 13, 2016); *see also, e.g.*, *Ziglar v. Abbasi*, 137 S. Ct. 1843, 1867 (2017). Plaintiff argues that the intra-corporate conspiracy doctrine does not apply only because the conspiracy she alleges "pre-dates" the individual Defendants' employment at DarkMatter and the individual Defendants worked with DarkMatter in furtherance of the alleged conspiracy when they were still employees of CyberPoint. (ECF 35, p. 34.)

The allegations in the Complaint do not support that assertion. The Complaint does not allege that any individual Defendant worked with DarkMatter in any capacity other than as a DarkMatter employee. Nor does the Complaint allege any period of time during which DarkMatter allegedly operated the cyber-surveillance program "Project Raven" while the individual Defendants worked on the program as CyberPoint employees. Instead, the Complaint alleges that the individual Defendants moved to DarkMatter at the same time DarkMatter took over the program from CyberPoint. (ECF 1 ¶ 67 (alleging that the individual Defendants "transitioned from CyberPoint to DarkMatter" "as part of th[e] effort" to "transition[] cyber services under Project Raven from CyberPoint to DarkMatter").)

Because the Complaint alleges that DarkMatter and the individual Defendants worked together solely as employer-employees, they could not conspire with one another as a matter of law. *See McGraw Co.*, 2016 WL 3745063, at *7. Consequently, Plaintiff's CFAA conspiracy claim fails.

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

A. Plaintiff Fails to Overcome The Presumption Against Extraterritoriality

Whether a claim is supported by sufficient connections to the United States to come within a federal court's jurisdiction under the ATS is a fact-based analysis. *Al Shimari v. CACI Premier Tech., Inc.*, 758 F.3d 516, 527 (4th Cir. 2014). Here, Plaintiff's ATS claim against the individual Defendants does not rest on alleged United States conduct sufficient to rebut the presumption against extraterritoriality. *See Nestlé USA, Inc. v. Doe*, 141 S. Ct. 1931, 1936 (2021) (requiring domestic conduct relevant to the "focus" of the ATS); *Kiobel v. Royal Dutch Petroleum Co.*, 569 U.S. 108, 124-125 (2013) ("[E]ven where the claims touch and concern the territory of the United States, they must do so with sufficient force to displace the presumption against extraterritorial application."). Plaintiff does not allege that she was surveilled in the United States or that any substantial part of the alleged cyber surveillance touched or concerned the United States. Again, Plaintiff alleges merely that the individual Defendants, while abroad, conducted cyber surveillance on behalf of a foreign government that targeted Plaintiff in the Middle East. (ECF 1 ¶¶ 20, 25-27, 116-123.)

Plaintiff endeavors to list out the individual Defendants' connections to the United States (ECF 35, pp. 35-36), but each item on that list is inapposite: item (i) relates to events *before* the individual Defendants were employed by DarkMatter—and those events (the alleged general development of cyber-surveillance technology) fall well beyond "the statute's focus," *Nestlé*, 141 S. Ct. at 1934; items (ii)-(v) & (vii) relate to the individual Defendants' alleged use of U.S. technology and personnel resources, not any ongoing connection to the United States; and items (vi) & (viii)-(x) rehash Plaintiff's trumped-up description of the alleged hack, with the fortuitous location of Apple's servers constituting the only connection to the United States. Plaintiff

identifies no case holding that such limited connections to the United States are enough for jurisdiction under the ATS.

Instead, Plaintiff relies on decisions involving far more extensive U.S. connections than alleged here. (ECF 35, pp. 36-37.) For example, *Al Shimari v. CACI Premier Technology, Inc.* involved allegations of torture at Abu Ghraib, Iraq, by employees of a *U.S. corporation* contracted by the *U.S. Department of Interior* (DOI) to interrogate prisoners held by the *U.S. military* in a *U.S. facility*, where the employees were issued security clearances by the *U.S. Department of Defense* and the contractor was paid based on invoices it mailed to *U.S. agency accounting offices*. 758 F.3d at 522, 528-529. In addition, managers of the contractor located in the United States allegedly were aware of the misconduct, encouraged it, and attempted to cover it up. *Id.* at 523, 529. In concluding that the plaintiffs' ATS claims came within the federal courts' jurisdiction, the Fourth Circuit held that "[t]he plaintiffs' claims reflect extensive 'relevant conduct' in United States territory." *Id.* at 528 (quoting *Kiobel*, 569 U.S. at 124). All of Plaintiffs' other authority is in the same vein. *See Jane W. v. Thomas*, 560 F. Supp. 3d 855, 878 (E.D. Pa. 2021) (defendant allegedly attacked a compound under the control of U.S. Agency for International Development and was deceptive about his role in the attack when he immigrated into the United States); *Sexual Minorities Uganda v. Lively*, 960 F. Supp. 2d 304, 310-311 (D. Mass. 2013) (although defendant's alleged "offensive conduct" against "LGBTI groups" had a "substantial focus on Uganda," both "defendant and his . . . conduct [we]re based in" Springfield, Massachusetts); *Estate of Alvarez v. Johns Hopkins Univ.*, No. TDC-15-0950, 2022 WL 1138000, *11 (D. Md. Apr. 18, 2022) (nonconsensual human medical experiments allegedly "were conceived, designed, and approved in the United States, by United States citizens working for both the United States government and United States institutions," such that "the tortious conduct was not a foreign-generated activity;

rather it was conduct allegedly perpetrated pursuant to a partnership between the United States government and a private entity which provided 'civilian contractors'"). Unlike in those cases, the alleged cyber surveillance here has no U.S. nexus: Plaintiff alleges that a foreign government both solicited the surveillance and used the information obtained from it.

Contrary to Plaintiffs' suggestion (ECF 35, p. 37), the Ninth Circuit did not convey that a minimal U.S. connection can suffice for jurisdiction under the ATS in *Mujica v. AirScan Inc.*, 771 F.3d 580, 594-595 (9th Cir. 2014). Rather, in explaining the *lack* of jurisdiction in that case—where the only U.S. connection was the defendant's U.S. citizenship—the court simply contrasted cases where "at least some of the conduct relevant to the[] claims occur[red] in the United States." *Id.* If there were any doubt, *Nestlé* subsequently emphasized that there is no ATS jurisdiction even where "defendant corporations allegedly made 'major operational decisions' in the United States." 141 S. Ct. at 1935. For allegations to "touch and concern" the United States with "sufficient force to displace the presumption against extraterritorial jurisdiction," *Kiobel*, 569 U.S. 108, 124-125, domestic conduct relevant to the "focus" of the statute—not mere peripheral or incidental conduct—is required, *Nestlé*, 141 S. Ct. at 1936-1937.

The Complaint here lacks allegations of sufficient U.S. connections to displace that presumption. The Court, therefore, lacks jurisdiction over Plaintiff's ATS claim. *See Nestlé*, 141 S. Ct. at 1936-1937.

B. Plaintiff Does Not Allege A Violation By The Individual Defendants That Is Actionable Under The ATS

The Complaint's factual allegations do not support Plaintiff's argument that the individual Defendants engaged in "persecution" that has been recognized as a crime against humanity and is actionable under ATS. The Complaint alleges that UAE officials, not the individual Defendants, "arrested" and "tortured" Plaintiff because of her human rights advocacy. (ECF 1 ¶¶ 122, 124.)

Plaintiff thus asks the Court to expand its "narrow" authority to create a cause of action under the ATS—which requires that the defendant violated an international law norm that is "specific, universal, and obligatory" and "'defined with a specificity comparable to' the three international torts known in 1789," *Nestlé*, 141 S. Ct. at 1938 (quoting *Sosa v. Alvarez-Machain*, 524 U.S. 692, 721, 725, 732 (2004))—to extend to allegedly providing cyber surveillance services to a foreign sovereign for the sovereign's use on its own soil. But Plaintiff identifies no support for that expansion.

Significantly, Plaintiff does not refute that her expansive theory would place this Court in the position of opining on the legality of a foreign sovereign's actions on its own soil, thereby risking potential foreign policy repercussions. The Supreme Court has stressed (i) "the need for judicial caution in considering which claims could be brought under the ATS, in light of foreign policy concerns," (ii) that such concerns "should make courts particularly wary of impinging on the discretion of the Legislative and Executive Branches in managing foreign affairs" in recognizing ATS claims, and (iii) that "[t]hese concerns, which are implicated in any case arising under the ATS, are all the more pressing when the question is whether a cause of action under the ATS reaches conduct within the territory of another sovereign." *Kiobel*, 569 U.S. at 116-117 (alterations and ellipses in original) (quoting *Sosa*, 524 U.S. at 727); *see also Broidy Cap. Mgmt., LLC v. State of Qatar*, 982 F.3d 582, 592 (9th Cir. 2020), *cert. denied sub nom. Broidy Cap. Mgmt., LLC v. Qatar*, 141 S. Ct. 2704 (2021); *accord Doe I v. Cisco Sys., Inc.*, No. 5:11-CV-02449-EJD, 2015 WL 5118004, at *4 (N.D. Cal. Aug. 31, 2015). Such potential impact on foreign policy is a "sound reason" why Congress "might doubt the efficacy or necessity" of the ATS remedy Plaintiff seeks against the individual Defendants, and thus precludes recognition of the cause of action Plaintiff seeks. *Nestlé*, 141 S. Ct. at 1938-1939 ("A court must not create a private right of action

if it can identify even one sound reason to think Congress might doubt the efficacy or necessity of the new remedy." (internal quotation marks and alterations omitted)).

Nor do Plaintiff's allegations support her argument that the individual Defendants facilitated "widespread" or "systematic" attacks. (ECF 35, p. 40.) While the Complaint alleges that the UAE targeted human rights advocates for persecution, the allegations tying the individual Defendants' alleged cyber surveillance to targeting of actual persons concern only three persons besides Plaintiff. (*Compare* ECF 1 ¶¶ 31-49 *with* ¶¶ 74-77.) The reporting from the U.S. Department of State and Amnesty International on the UAE and Saudi Arabia described in the Complaint does not address any cyber surveillance. (*Id.* ¶¶ 34-37, 44.) And the Complaint's assertion that the alleged cyber surveillance program "allowed" operatives to hack into hundreds of iPhones does not support the inference that the UAE took systematic action against the owners of those phones. (*Id.* ¶ 82.)

Plaintiff thus alleges far fewer instances of persecution using cyber surveillance than were found insufficient to support jurisdiction in *Mamani v. Berzain*, 654 F.3d 1148 (11th Cir. 2011). *Mamani* held that allegations of 70 persons killed and approximately 400 persons injured was not a scale of loss "sufficiently widespread . . . to amount definitely to a crime against humanity under already established international law." *Id.* at 1156. Plaintiff ignores that conclusion in suggesting, without citation, that *Mamani* indicates a small number of victims can establish a crime against humanity. (*See* ECF 35, p. 42, n.11.)

Simply put, the Complaint alleges no basis for construing Plaintiff's claim as fitting within the "narrow" class of claims actionable under the ATS.

IV. DEFENDANTS ARE ENTITLED TO CONDUCT-BASED IMMUNITY

Plaintiff's allegations that Defendants acted on behalf of the UAE, which must be taken as true, show that they are entitled to conduct-based immunity. (ECF 1 ¶¶ 1, 60-77, 113.) As for the

individual Defendants, Plaintiff emphasizes that the U.S. State Department has not filed a suggestion of immunity (ECF 35 pp. 43-44), but *Samantar v. Yousuf* makes clear that the district court has authority to decide a question of immunity for itself, *see* 560 U.S. 305, 311-312 (2010). Plaintiff also suggests that only foreign officials are entitled to conduct-based immunity, but fails to address the authorities supporting application of immunity based on allegations like these. (*See* ECF 28, p. 27 (citing, *e.g., Butters v. Vance Int'l, Inc*., 225 F.3d 462, 466 (4th Cir. 2000) (noting that "courts have extended derivative immunity to private contractors"); *Broidy Cap. Mgmt. LLC v. Muzin*, 12 F.4th 789, 802 (D.C. Cir. 2021) (considering affording such immunity)).)

As for DarkMatter, the petition for certiorari by the appellees in *NSO Grp. Technologies Ltd. v. Whats App Inc.*, No. 21-1338 (U.S. Apr. 8, 2022)—which concerns whether a private *entity* may be entitled to conduct-based immunity—remains pending. Indeed, the Supreme Court has called for the views of the Solicitor General on that question. *See* No. 21-1338 (U.S. June 6, 2022) (https://www.supremecourt.gov/search.aspx?filename=/docket/docketfiles/html/public/21-1338.html). DarkMatter has thus preserved its common-law immunity argument.

V. THE COURT SHOULD DENY LEAVE TO AMEND

District courts may deny leave to amend "where the amendment would be futile." *Thinket Ink Info Res., Inc. v. Sun Microsystems, Inc.*, 368 F.3d 1053, 1061 (9th Cir. 2004). That is the case here. Plaintiff's allegations establish an absence of both any harm felt in the United States and express aiming (as the hacking scheme's sole alleged connection to the United States is the location of Apple's servers). *See* pp. 7-12, supra. Because Plaintiff's allegations (i) affirmatively establish that this Court lacks personal jurisdiction, (ii) fail to state a CFAA claim, and (iii) fail to state an ATS claim over which this Court has jurisdiction, the Court should dismiss all of her claims with prejudice.

CONCLUSION

For the foregoing reasons, the complaint should be dismissed with prejudice.

Respectfully submitted,

Dated: September 9, 2022

AKIN GUMP STRAUSS HAUER & FELD LLP

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

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

SCHWABE, WILLIAMSON & WYATT, P.C.

s/ Nika Aldrich
Nika Aldrich, OSB No. 160306
naldrich@schwabe.com
Telephone: 503-222-9981

ATTORNEYS FOR DEFENDANT DARKMATTER GROUP

SNELL & WILMER L.L.P.

s/ Clifford S. Davidson

Clifford S. Davidson, OSB No. 125378
csdavidson@swlaw.com
Telephone: 503-624-6800

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