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.
601 SW 2nd Ave., Suite 2000
Portland, OR 97204
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' REPLY IN SUPPORT OF JOINT MOTION TO DISMISS FIRST AMENDED COMPLAINT** **REQUEST FOR ORAL ARGUMENT**

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

INTRODUCTION

The question presented is whether the sporadic connections Plaintiff alleges permit her to sue Defendants in the United States. The answer is no. Plaintiff cannot show that the foreign *Defendants* purposefully directed their conduct towards the United States based on the foreign *Plaintiff*'s unilateral travel here. Although Plaintiff relies heavily on a recent Ninth Circuit decision indicating that courts may consider both purposeful availment and purposeful direction analyses in appropriate cases, that same decision—which held that purposeful availment was *lacking*—only reinforces that this Court lacks jurisdiction over Defendants. Otherwise, Plaintiff continues to rely on third-party, historical, and attenuated contacts that do not arise out of or relate to her claims. And Plaintiff fails to overcome this Court's prior determination that exercising jurisdiction over Defendants would be unreasonable.

Nor has Plaintiff stated claims under the Computer Fraud and Abuse Act (CFAA) and Alien Tort Statute (ATS). Plaintiff's view that the CFAA applies to *any* hack of *any* smartphone connected to the internet—no matter where the alleged hacker and device are located—flouts the statutory text and turns the presumption against extraterritoriality on its head. Regardless, Plaintiff has not plausibly alleged a loss or physical injury under the CFAA. And Plaintiff's ATS claim likewise falls outside the statute's territorial and substantive limits.

The Court should dismiss Plaintiff's Amended Complaint—this time with prejudice.

ARGUMENT

I. THE COURT LACKS PERSONAL JURISDICTION OVER ALL DEFENDANTS

Because Plaintiff does not dispute that Defendant Ryan Adams is domiciled abroad, the personal jurisdiction analysis hinges on whether Plaintiff's allegations as to each Defendant satisfy

Rule 4(k)(2) of the Federal Rules of Civil Procedure. (*See* ECF 63 at 19 n.5.)[1] This Court has already held that the purposeful direction test, not the purposeful availment test, dictates whether Plaintiff's allegations satisfy the U.S. Constitution. (*See* ECF 44 at 9.)

Despite acknowledging that "the 'purposeful direction' test 'typically' applies to tort claims," the Ninth Circuit recently observed that "courts should comprehensively evaluate the extent of the defendant's contacts with the forum," "which *may* mean looking at both purposeful availment and purposeful direction." *Davis v. Cranfield Aerospace Sols., Ltd.*, 71 F.4th 1154, 1162 (9th Cir. 2023) (emphasis added) (quoting *Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme*, 433 F.3d 1199, 1206 (9th Cir. 2006) (en banc)). But unlike here, the tort at issue in *Davis* centered on an underlying contractual relationship.[2] Thus, while the court found it "appropriate to look at both approaches" in that contract-adjacent context, it did not state that doing so is always required. *Id.* Nor did it say it was appropriate to do so where, as here, the purposeful availment factors—such as a "contract's negotiations, terms, [and] contemplated consequences," along with the parties' "course of dealing," *id.* at 1163—are plainly inapt.

Regardless, Defendants lack the requisite minimum contacts with the United States under either framework. Moreover, all seven reasonableness factors weigh against exercising jurisdiction.

---

[1] Any general allegations about DarkMatter may not be attributed to the individual Defendants. And allegations that apply only to the individual Defendants (such as allegations concerning the Deferred Prosecution Agreement (DPA)) may not be attributed to DarkMatter. *See Rush v. Savchuk*, 444 U.S. 320, 331-332 (1980) ("aggregating" defendants in this manner is "plainly unconstitutional").

[2] The *Davis* plaintiffs represented persons who died in an airplane crash. 71 F.4th at 1159-1160. A company located in Idaho (the forum) had designed an allegedly defective airplane component. *Id.* at 1160. The defendant was an English company that contracted with the Idaho company to help the Idaho company obtain safety certifications for the component. *Id.*

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

Plaintiff cannot pass the "purposeful direction" test, which "generally appl[ies]" to "claims sounding in tort," *Picot v. Weston*, 780 F.3d 1206, 1212 (9th Cir. 2015), because she fails to adequately allege that Defendants expressly aimed tortious conduct at the United States or caused harm they knew she would likely suffer there.

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

By any measure, Plaintiff does not allege that Defendants "aim[ed]" any tort-related conduct at the United States. *See AMA Multimedia, LLC v. Wanat*, 970 F.3d 1201, 1209 n.5 (9th Cir. 2020). Plaintiff's main new allegation—that she traveled to the United States with her phone for five days in 2017 after it was allegedly hacked—cannot establish express aiming because "the 'unilateral activity' of a plaintiff" cannot support jurisdiction, and Plaintiff would have experienced the same harm "wherever else [she] might have traveled." *Walden v. Fiore*, 571 U.S. 277, 286, 290 (2014) (quoting *Burger King v. Rudzewicz*, 471 U.S. 462, 475 (1985)).

Plaintiff seeks to avoid *Walden*'s focus on "intentional conduct by *the defendant*," 571 U.S. at 286 (emphasis added), through a linguistic sleight of hand. She argues that because Plaintiff visited the United States, Defendants "accesse[d]" her phone "in the forum to commit a tort." (ECF 70 at 18.) But the amended complaint alleges that Defendants accessed Plaintiff's phone when it was located *outside* the forum, *then* Plaintiff carried the phone into the forum as the device "continuously transmit[ted] data." (ECF 54 ¶ 127; *see id.* ¶ 150 (information-and-belief allegation that Defendants exfiltrated data in U.S. "due to the continuous and ongoing hack")); *cf. Nollan v. California Coastal Comm'n*, 483 U.S. 825, 838 (1987) (rejecting an argument that "essentially turns on a play on the word 'access'"). If a tortfeasor sent a package containing poison to a

recipient in California, and the recipient opened the package after driving to Oregon, the tortfeasor did not thereby "aim" his conduct at Oregon.

While admitting that "Defendants did not control [her] travel," Plaintiff argues that Defendants "did control their own actions taken after they knew she traveled." (ECF 70 at 18.) But Plaintiff alleges no such "actions." Plaintiff implies that Defendants expressly aimed their conduct at the United States because Defendants did not engage in *additional* conduct to cease the alleged flow of information from her device as she unilaterally traveled there. But relying on Plaintiff's own "forum connections" in this manner would "impermissibly allow[] a plaintiff's contacts with the defendant and forum to drive the jurisdictional analysis." *Walden*, 571 U.S. at 289. And even if DarkMatter knew about Plaintiff's trip—something Plaintiff never squarely alleges (*see* ECF 70 at 10 (arguing Defendants "would have known"))—"knowledge of [a plaintiff's] strong forum connections" does not "satisf[y] the 'minimum contacts' inquiry." *Walden*, 571 U.S. at 289 ("Petitioner's actions in Georgia did not create sufficient contacts with Nevada simply because he allegedly directed his conduct at plaintiffs whom he knew had Nevada connections.").

For all those reasons, Plaintiff's authorities involving hacks of in-forum devices and forum residents are inapposite. *See DEX Sys., Inc. v. Deutsche Post AG*, 727 F. App'x 276, 278 (9th Cir. 2018); *Felland v. Clifton*, 682 F.3d 665, 676 n.3 (7th Cir. 2012); *MacDermid, Inc. v. Deiter*, 702 F.3d 725, 730 (2d Cir. 2012); *Climax Portable Machine Tools, Inc. v. Trawema GmbH*, No. 3:18-cv-1825-AC, 2020 WL 1304487 (D. Or. Mar. 19, 2020); *NetApp, Inc. v. Nimble Storage, Inc.*, 41 F. Supp. 3d 816, 826 (N.D. Cal. 2014). Indeed, the Ninth Circuit has indicated that even a server's location in the forum *at the time it is initially accessed* "is insufficient to establish personal jurisdiction." *Will Co., Ltd. v. Lee*, 47 F.4th 917, 926 (9th Cir. 2022) (citing *Hungerstation LLC v.*

Fast Choice LLC, 857 F. App'x 349, 351 (9th Cir. 2021) (the Ninth Circuit "has never decided that personal jurisdiction is proper over a private foreign entity solely because that entity … remotely access[ed] servers located in the United States")).

Plaintiff's attempt to distinguish *Hungerstation* is unavailing. In arguing that she "specifically chose to use an iPhone because of its security and knowledge that it relied on servers located in the United States" (ECF 70 at 20), Plaintiff "improperly attributes" her own forum connections "to the defendant." *Walden*, 571 U.S. at 289. And in arguing that DarkMatter allegedly "chose to hack her otherwise secure iPhone … [using] Apple's U.S. servers" (ECF 70 at 20), Plaintiff ignores this Court's statement that this allegation, "at most, shows that 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." (ECF 44 at 13.)

Plaintiff also attempts to rely on additional third parties' forum connections. For example, she cites Defendants' allegedly "deliberate choice to use U.S.-based anonymization services and proxy servers." (ECF 70 at 19.) But such allegations—concerning third-party technology companies' fortuitous locations—do not show that DarkMatter directed its conduct at the United States. As this Court already explained, "the choice by a third party to operate … in the forum is insufficient to show that a foreign defendant … purposefully directs their actions at the forum." (ECF 44 at 15.) That is why in *AMA*, the Ninth Circuit held there was no express aiming despite the defendant's purchase of proxy domains and DNS services from American companies. 970 F.3d at 1209. (*See also* ECF 63 at 10-11 (discussing *AMA* in detail).)[3] And unlike cases where

[3] Although *AMA* forecloses Plaintiff's jurisdictional argument, Plaintiff highlights its discussion of a defendant's "rel[iance] on U.S.-based servers." (ECF 70 at 19 (citing *AMA*, 970 F.3d at 1212 n.8).) But *AMA* referenced "U.S.-based servers" while distinguishing (on multiple grounds) a case where the defendant himself operated websites using "servers physically located in Virginia." *UMG Recordings, Inc. v. Kurbanov*, 963 F.3d 344, 349 (4th Cir. 2020). In that case,

defendants targeted servers due to their U.S.-connections in order to "overcome" or "circumvent" blacklist restrictions, among many other forum connections not present here (ECF 70 at 19),[4] Plaintiff does not contend that the alleged location of the anonymization services and proxy servers in the United States (versus anywhere else) mattered to Defendants. Along the same lines, by invoking Plaintiff's communications with "U.S. journalists, NGOs, and human rights advocates" (ECF 70 at 20), Plaintiff impermissibly relies on her own connections with third parties who, in turn, have connections with the United States—not *Defendants'* forum connections.

2. Defendants' Alleged Conduct Did Not Cause Harm That Defendants Knew Would Likely Be Suffered In The United States

Defendants did not purposefully direct their conduct at the United States for another, independent reason: Their alleged actions were not "performed for the very purpose of having their consequences felt in the 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.) (quoting *Brainerd v. Governors of the Univ. of Alberta*, 873 F.2d 1257, 1260 (9th Cir. 1989)), *aff'd*, No. 22-35107, 2022 WL 16958933 (9th Cir. Nov. 16, 2022).

---

the Fourth Circuit noted that even such conduct—which is lacking here—may not have been "sufficient to confer specific personal jurisdiction." *Id.* at 354. Jurisdiction was proper given "other jurisdictionally relevant facts." *Id.*

[4] In *HB Prods., Inc. v. Faizan*, 603 F. Supp. 3d 910 (D. Haw. 2022), and *42 Ventures, LLC v. Mav*, No. 20-cv-00228, 2022 WL 2400030 (D. Haw. June 15, 2022), the defendants also "host[ed] … infringing websites and apps on servers located in the United States," and used those websites to "distribute[] pirated copies of motion pictures … to individuals in the United States." *Id.* at *4; *accord HB Prods.*, 603 F. Supp. 3d at 918-919 (D. Haw. 2022). Indeed, the defendants used U.S. servers in part to "increase the service speed to users visiting these websites from the United States." *42 Ventures*, 2022 WL 2400030, at *4; *accord HB Prods.*, 603 F. Supp. 3d at 930. For those and other reasons, all of which are inapplicable here, the courts found that the tortious infringement at issue "occurred in the United States." *42 Ventures*, 2022 WL 240030, at *4; *HB Prods.*, 603 F. Supp. 3d at 930.

Plaintiff does not seriously contend otherwise. She repeats that Defendants "*knew* her device was in the United States" after she voluntarily traveled there. (ECF 70 at 21.) As already discussed, even if supported by Plaintiff's complaint, that is irrelevant. Plaintiff also argues that Defendants knew she would suffer harm in the United States because she used her phone to communicate with U.S. persons. (ECF 70 at 22.) But, again, "this element" examines "the foreseeability of harm caused *in the forum to the plaintiff*," not the plaintiff's connections with third parties who happen to live in the forum. (ECF 44 at 17 (emphasis added) (citing *Burri Law PA v. Skurla*, 35 F.4th 1207, 1216 (9th Cir. 2022); *Dole Food Co. v. Watts*, 303 F.3d 1104, 1113 (9th Cir. 2002)).) Plaintiff cites no authority for this argument, and for good reason: If she is correct, any alleged hacking victim who communicates with U.S. residents could purport to suffer harm in the United States without setting foot here.

At any rate, 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 v. Jones*, 465 U.S. 783, 789 (1984)). Even if Plaintiff was in the United States during some brief period when some of her data was exfiltrated (ECF 70 at 21-22), Plaintiff—who "did not discover" the hack until reading Reuters reporting years after leaving the United States (ECF 54 ¶ 155)—could not have "felt" harm in the forum because she experienced no "consequences" there. *Brown*, 2022 WL 43880, at *3; *see also Yahoo!*, 433 F.3d at 1206 (harm must be "*felt* … within" the forum (emphasis added)). If such U.S. harm is cognizable at all, it is at least not "jurisdictionally sufficient." (ECF 44 at 16); *see also Dole Food Co.*, 303 F.3d at 1111 (harm must be jurisdictionally "significant"). Accordingly, Plaintiff cannot satisfy either prong of the purposeful direction test.

B. Defendants Did Not Purposefully Avail Themselves Of The Privilege Of Conducting Activities In The United States

Assuming that a purposeful availment analysis is relevant here, it "leads to the same result." *Davis*, 71 F.4th at 1163. Purposeful availment "exists when a defendant's dealings with a [forum] establishes a 'quid pro quo'—where the defendant 'purposefully avails itself of the privilege of conducting activities within the forum … , thus invoking the benefits and protections of its laws,' and in return 'submit[s] to the burdens of litigation' in the [forum]." *Id.* (quoting *Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 802 (9th Cir. 2004)). That typically occurs in actions involving contract-related claims, where the inquiry is whether a defendant deliberately "exploit[ed] a market in the forum … or enter[ed] a contractual relationship centered there." *Id.* (quoting *Yamashita v. LG Chem, Ltd.*, 62 F.4th 496, 503 (9th Cir. 2023)).

Of course, the purposeful availment framework is not an exception to the "[w]ell-established principles of personal jurisdiction" set forth in *Walden*. 571 U.S. at 291. "The proper focus of the 'minimum contacts' inquiry in intentional-tort cases is 'the relationship among the defendant, the forum, and the litigation.'" *Id.* (quoting *Calder*, 465 U.S. at 788). No matter which Ninth Circuit test is at play, "it is the defendant, not the plaintiff or third parties, who must create contacts with the forum." *Id.* Thus, as with purposeful direction, "[t]he unilateral activity of another party" cannot support purposeful availment. *Davis*, 71 F.4th at 1163 (internal quotation marks omitted).

Accordingly, Plaintiff's purposeful availment theory fails for the same reasons as her purposeful direction theory. Defendants (besides having no contractual relationship with Plaintiff) did not reach into the United States, invoke the benefits and protections of U.S. law, or submit to the burdens of litigating in the United States, by allegedly sending an iMessage to a phone located abroad or otherwise. As discussed above, Plaintiff's primary counterargument—that her phone

was "located in the United States" for a five-day period after it had allegedly been hacked (ECF 70 at 14)—hinges on her own "unilateral activity." *Davis*, 71 F.4th at 1163. And Plaintiff's recycled arguments about Apple and other technology companies impermissibly rely on third parties' contacts. (*See* ECF 70 at 16.)

Straining to bypass *Walden*, Plaintiff cherry-picks language from *Freestream Aircraft (Bermuda) Ltd. v. Aero Law Grp.*, 905 F.3d 597, 606 (9th Cir. 2018), to argue that she has alleged a "tort within the forum," which "usually supports the exercise of personal jurisdiction." (ECF 70 at 14.) But *Freestream* referred to "an alleged tort committed while the defendant was *physically present* in the forum," and expressly distinguished "defendant[s] who never physically entered the forum." 905 F.3d at 604, 605 (emphasis added). A defendant who "voluntarily entered a [forum]" to commit a tort can be said to have "invoked the protections of its laws." *Id.* at 606 (quotation omitted). As Defendants have pointed out (and Plaintiff does not address), *Calder* and *Walden* make clear that the abstract location of an intentional tort is *not* dispositive when the alleged tortfeasor remains physically outside the forum. (*See* ECF 63 at 7 n.1.)

Finally, Plaintiff purports to rely on Defendants' "entire course of dealing." (ECF 70 at 16 (quoting *Davis*, 71 F.4th at 1163).) To be sure, "the parties' actual course of dealing" may be relevant to whether a defendant "received fair notice … that he might be subject to suit in [the forum]," as in the context of a voluntarily contractual relationship. *Burger King*, 471 U.S. at 480, 487; *see also Global Commodities Trading Grp., Inc. v. Beneficio de Arroz Choloma, S.A.*, 972 F.3d 1101, 1108-1109 (9th Cir. 2020) (based on parties' "lengthy and ongoing course of dealing," it was "reasonable for [the defendant] to expect that it would be haled into court in [the forum]"). That flows from general contract principles: The "intention[s]" of "parties to a promise or

agreement," including any intention to invoke the benefits and protections of a forum's laws, may be evidenced by a contractual "course of dealing." Restatement (Second) of Contract § 202(5).

But even when such a "course of dealing" inquiry makes sense, significant dealings with the forum may not be enough to show purposeful availment. In *Davis*, the defendant's employees "engaged in several telephone calls, emails, and other correspondence with individuals in [the forum]," provided forum-residents with "technical advice and assistance and helped them develop procedures and analysis to obtain … certifications" that were central to the plaintiff's claims, and even took "two trips" to the forum "as part of the contract" at issue. 71 F.4th at 1164-1165. Yet that conduct was not "so substantial or widespread that it reflect[ed] [an] attempt to gain the benefits and protections of the forum." *Id.* at 1166 (internal quotation marks omitted). "[O]ut-of-state contacts by mail and phone and payments sent from [the] forum … [do] not establish 'the deliberate creation of a substantial connection' with the forum." *Id.* at 1165 (quoting *Sher v. Johnson*, 911 F.2d 1357, 1362 (9th Cir. 1990)). And travel to the forum does not establish purposeful availment when the forum does not hold a "special place" in the parties' relationship. *Id.*

If those contacts were too "attenuated," *Davis*, 71 F.4th at 1165, Defendants' far weaker contacts are too. Plaintiff argues that "DarkMatter [allegedly] recruited individuals with U.S. security clearances," "transferred technology … protected by U.S. export licenses," and "purchased specialized exploits … [from] two U.S. companies." (ECF 70 at 16.) But such technology was allegedly "altered in significant ways before being deployed." (ECF 44 at 19; *see, e.g.*, ECF 54 ¶ 93 ("upgrade"), ¶ 105 ("enhance").) Beyond that, nothing about Defendants' alleged role in these transactions with third parties reflects an expectation or intent that Defendants would "be subject to suit in [the forum]" based on their future alleged use of that modified

technology abroad. *Burger King*, 471 U.S. at 487. If such attenuated contacts were enough for purposeful availment, U.S. courthouse doors would be flung open to foreign plaintiffs suing foreign entities that merely purchased technology from U.S. companies like IBM and Microsoft. In any event, *Davis* makes clear that "course of dealing" allegations must still "relate[] to" a plaintiff's claims. 71 F.4th at 1162, 1163. As discussed next, these allegations do not.

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

Most of the purported U.S. contacts that Plaintiff cites are not sufficiently connected to her claims. *See Ford Motor Co. v. Montana Eighth Judicial Dist. Ct.*, 141 S. Ct. 1017, 1025 (2021) (claims must "arise out of or relate to" Defendants' contacts). Contacts that lack a "direct nexus … [to] the cause of action" or a "close connection" to the alleged "injury" do not count. *Yamashita v. LG Chem, Ltd.*, 62 F.4th 496, 504 (9th Cir. 2023). Plaintiff's allegations about DarkMatter's general history, corporate acquisitions, and hiring and marketing practices are thus irrelevant. *See id.* at 505-506. Further, as this Court held (and Plaintiff does not dispute), the allegation "that Defendants may have developed expertise and knowhow in the forum that was later used to create the malware that infected Plaintiff's phone is not enough to confer jurisdiction." (ECF 44 at 19.) And by relying on Defendants' alleged "acquisition," "transferring," and "leveraging" of U.S. companies' technology (ECF 70 at 23-24), Plaintiff asks this Court to "impart the affiliation between … third part[ies] and the forum to Defendants." (ECF 44 at 18.)

At bottom, Plaintiff believes that "*[e]very* U.S. contact alleged" is relevant, because every allegation purportedly "relates to Defendants' development and installation of the very exploit used to exfiltrate data from Alhathloul[']s device." (ECF 70 at 23-24.) But Plaintiff fails to square that conclusory argument with the Supreme Court's admonition that this prong "incorporates real limits." (ECF 44 at 18 (quoting *Ford*, 141 S. Ct. at 1026).) Defendants' attendance at a

cybersecurity conference, for example, cannot possibly fit within those limits. (ECF 54 ¶ 7.) Nor does Plaintiff defend the consequences of her theory, which would make U.S. courts a universal forum for "foreign-cubed" litigation, *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" to the United States based on remote history and happenstance.

D. Exercising Jurisdiction Over Defendants Would Be Unreasonable

This Court previously held that "[e]ven if Plaintiff had shown that Defendants had sufficient 'minimum contacts' with the United States … this Court would still find that the exercise of jurisdiction over Defendants would be unreasonable." (ECF 44 at 22-23.) Plaintiff seeks to overcome that conclusion by leveraging three of the seven reasonableness factors across the entire analysis. But each factor counts only once. And Plaintiff does not meaningfully address Defendants' updated showing that *every* factor supports Defendants. (*See* ECF 63 at 18-19.)

First Factor. As this Court has explained, allegedly "sending 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' into the United States' affairs." (ECF 44 at 20.) Plaintiff's new allegation that she brought her phone to the United States for a few days after the alleged hack, which allegedly revealed "her communications with U.S. individuals and her affairs in the forum" (ECF 70 at 24), does not change this Court's conclusions that the alleged conduct was "aimed at a nonresident" located abroad and had only a fortuitous connection to the forum. (ECF 44 at 20.)

Second Factor. Plaintiff's scattershot arguments that this case involves "only a minimal [litigation] burden" miss the mark. (ECF 70 at 24.) Adopting Plaintiff's contention that retaining "U.S. counsel" to defend against lawsuits like this one diminishes a defendant's due process rights (ECF 70 at 24-25) would plainly "offend traditional conception[s] of fair play and substantial

justice." *Burger King*, 471 U.S. at 464 (internal quotation marks omitted). Plaintiff relies on a single, non-binding decision that notes a defendant's U.S. counsel in passing while emphasizing the defendant's extensive U.S. presence and "routine[]" engagement with the U.S. legal system. *In re ZF-TRW Airbag Control Units Prods. Liability Litig.*, 601 F. Supp. 3d 625, 703-704 (C.D. Cal. 2022). By contrast, Plaintiff points to Defendants' alleged marketing activities, i.e., DarkMatter's attendance at an annual conference from 2016 to 2019. (ECF 70 at 25 (citing ECF 54 ¶ 7).) That is not probative of Defendants' litigation burden, and the fact that DarkMatter "recently defended another case in U.S. courts" is even less so. (ECF 70 at 25.) As DarkMatter pointed out (and Plaintiff does not address), Plaintiff is alluding to a case that was dismissed *for lack of personal jurisdiction*. (ECF 63 at 18 (discussing *Oueiss v. Saud*, No. 1:20-cv-25022, 2022 WL 1311114, at *20-21 (S.D. Fla. Mar. 29, 2022).) Finally, by invoking the purported unavailability of "a fair trial in the UAE," Plaintiff improperly double counts (and misstates) the seventh factor, the existence of an alternative forum. (ECF 70 at 25.)

Third Factor. In Plaintiff's view, finding a conflict with the sovereignty of the UAE and Saudi Arabia would mean that "no private company working for a foreign government could be liable for its conduct." (ECF 70 at 25.) But this suit does not allege that Defendants merely happened to work for the UAE; it alleges that Defendants "*conspired with* … the UAE to persecute [Plaintiff]." (ECF 54 ¶ 231.) This Court rejected Plaintiff's prior attempt to obscure "the implications of this suit" given Plaintiff's grave allegations involving "conduct carried out at the behest of the UAE government." (ECF 44 at 21; *see also* ECF 71 at 6-7 (Amici arguing that DarkMatter acted "at the behest of the UAE and other regimes in the Middle East," and emphasizing "important transnational implications").) That reasoning still applies. Plaintiff does not dispute that her allegations also implicate the Saudi government. (ECF 54 ¶ 169 (allegation of

a Saudi "sham trial").) Both governments' "procedural and substantive interests" against a foreign court adjudicating such allegations are clear. *Asahi Metal Indus. Co., Ltd. v. Super. Ct. of Cal.*, 480 U.S. 102, 115 (1987). Comity points the same way: accepting Plaintiff's view would imply that "other nations" could "hale our citizens into their courts" to adjudicate claims alleging unlawful surveillance by the U.S. government in the United States. *Kiobel v. Royal Dutch Petroleum Co.*, 569 U.S. 108, 124 (2013). Finally, in arguing that "the U.S.'s interests" in enforcing federal statutes override these sovereignty concerns (s*ee* ECF 70 at 26), Plaintiff double counts both the fourth and sixth factors (as she perceives them).

Fourth Factor. In any event, this Court already found "that the fourth factor—the forum's interest in adjudicating the dispute—weighs against the exercise of jurisdiction." (ECF 44 at 21.) Plaintiff argues otherwise based on the same DPA and federal claims that were before the Court last time—and offers no reason why the Court should change its conclusion. (*See* ECF 70 at 26.)[5]

Fifth Factor. Similarly, this Court has already found "that the United States would not offer the most efficient judicial resolution for the controversy," while rejecting Plaintiff's arguments about the locations of "Apple's technology experts and the companies that [allegedly] designed and sold the exploits." (ECF 44 at 22.) Otherwise, all Plaintiff can muster is that "this factor is no longer weighed heavily." (ECF 70 at 27 (citing *Panavision Int'l, L.P. v. Toeppen*, 141 F.3d 1316, 1323 (9th Cir. 1998)).) But Plaintiff fails to show that this case involves the "limited amount of evidence and few potential witnesses" at issue in *Panavision*. 141 F.3d at 1323-1324.

Sixth Factor. Plaintiff circularly maintains that because her claims arise under federal law, the United States is most likely to provide convenient and effective relief. (ECF 70 at 27.) That

[5] Amici, for their part, point to general executive branch statements about spyware. (*See* ECF 71 at 14-15.) But the United States has various tools at its disposal to combat spyware; such statements do not indicate that U.S. courts have an interest in adjudicating *this* dispute.

is not the test. Plaintiff must 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 (sixth factor favored defendants despite claims arising under federal statutes). Plaintiff does not attempt to make that showing. Instead, she (again) folds the seventh factor into this one. (*See* ECF 70 at 27 (arguing the United States is a convenient and effective forum because Plaintiff should not have to "bring claims in the courts of" Saudi Arabia and the UAE).)

Seventh Factor. When the time comes to apply the seventh factor, Plaintiff misconstrues it. She continues to argue "that the UAE is not a viable alternative forum" (ECF 70 at 27), without attempting to satisfy her burden of proving the unavailability of any other alternative forum, including other countries or multinational tribunals that might have more interest than the United States in redressing Plaintiff's claimed injuries. (*See* ECF 63 at 19.) For example, one of amici's citations reflects that proceedings "related to mercenary spyware" are ongoing in numerous tribunals around the world. (ECF 71 at 13 n.53 (citing Citizen Lab, "Litigation and other formal complaints related to mercenary spyware" (updated July 31, 2023) (listing proceedings))[6].)

In sum, every factor weighs against exercising jurisdiction over Defendants. But even if this Court finds that several factors favor Plaintiff (or are neutral), the balance of the "reasonableness factors weigh against jurisdiction." (ECF 44 at 22-23.) When the Supreme Court emphasized that "[t]he unique burdens placed upon one who must defend oneself in a foreign legal system should have significant weight," and cautioned that "[g]reat care and reserve should be

[6] https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/.

exercised when extending our notions of personal jurisdiction into the international field," it was referring to cases like this one. *Asahi*, 480 U.S. at 114-115.

E. Plaintiff Is Not Entitled To Jurisdictional Discovery

Plaintiff purports to "reserve[] the right to seek jurisdictional discovery" at some future date if "Defendants contend that there is insufficient detail pled to support these or any other factual allegations or reasonable inferences." (ECF 70 at 12.) But such discovery is appropriate only "where pertinent facts bearing on the question of jurisdiction are controverted or where a more satisfactory showing of the facts is necessary." *Boschetto v. Hansing*, 539 F.3d 1011, 1020 (9th Cir. 2008) (quoting *Data Disc, Inc. v. Systems Tech. Ass'n*, 557 F.2d 1280, 1285 n.1 (9th Cir. 1977)). Defendants have accepted the truth of all non-conclusory allegations for purposes of this Court's personal jurisdiction analysis—but those allegations nevertheless fail to establish jurisdiction. To the extent Plaintiff moves for jurisdictional discovery so that she can assert *additional* allegations, Plaintiff may not obtain discovery based on a "hunch that it might yield jurisdictionally relevant facts" that "neither [her] complaint nor [any] affidavit allege." *Id.*

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

The Court alternatively may dismiss the Amended Complaint for failure to state a claim upon which relief can be granted. Plaintiff has not pleaded 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

According to Plaintiff, the CFAA has no real territorial limits with respect to the devices it protects *or* the conduct it prohibits. In her view, the CFAA applies to *any* alleged hack of *any*

phone that connects to the Internet—no matter how the phone is used or where the alleged hacker is located. That is doubly wrong.

First, the CFAA does not protect every device in the world with an internet connection. (ECF 70 at 28.) To be sure, the CFAA protects some devices "located outside the United States"—but such devices must be "used in or affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B). A connection to the Internet is not enough: Foreign commerce does not "mean literally all commerce occurring abroad," but only such commerce "directly involving the United States." *RJR Nabisco*, 579 U.S. at 344. By the same token, "foreign communication" means communication "directly involving the United States." *See* Antonin Scalia & Bryan Garner, READING LAW: THE INTERPRETATION OF LEGAL TEXTS 170 (2012) ("A word or phrase is presumed to bear the same meaning throughout a text[.]"). A random internet connection in Saudi Arabia or the UAE—without more—does not "directly involv[e]" the United States.

Plaintiff cites no authority that supports her interpretation of "protected device." Instead, she relies on decisions addressing devices that were connected to the Internet *within the United States* at the time of the unauthorized access, i.e., devices that were clearly used in "interstate commerce" and "interstate communication." *United States v. Trotter*, 478 F.3d 918, 921 (8th Cir. 2007) (defendant accessed U.S. non-profit's computer network); *see also Mifflinburg Telegraph, Inc. v. Criswell*, 277 F. Supp. 3d 750, 791-794 (M.D. Pa. 2017) (defendant accessed emails on computer located in Pennsylvania); *Property Rights Law Grp., P.C. v. Lynch*, No. 13-00273, 2014 WL 2452803, at *14 (D. Haw. May 30, 2014) (defendants accessed "cloud platform" based in United States). No court has embraced Plaintiff's near-limitless definition of "protected device"; this Court should not be the first.

Second, Plaintiff does not even try to argue that the CFAA's text "affirmatively and unmistakably … appl[ies] to foreign conduct." *Abitron Austria GmbH v. Hectronic Int'l, Inc.*, 600 U.S. 412, 417-418 (2023) (quoting *RJR Nabisco*, 579 U.S. at 335, 337). Instead, Plaintiff assumes that because the CFAA applies to some foreign "devices," the CFAA must *also* apply to all foreign "conduct." (ECF 70 at 29.) But the fact that a law "applies abroad" in one specific sense (*id.* (quoting *In re Apple Inc. Device Performance Litig.*, 347 F. Supp. 3d 434, 448 (N.D. Cal. 2018)), does not mean the law applies to foreign conduct. "[W]hen a statute provides for *some* extraterritorial application, the presumption against extraterritoriality operates to limit that provision to its terms." *See Morrison v. National Australia Bank Ltd.*, 561 U.S. 247, 265 (2010) (emphasis added). For example, the Supreme Court has "repeatedly held that even statutes … that expressly refer to '*foreign* commerce'… are not extraterritorial" with respect to the conduct they cover. *Abitron*, 600 U.S. at 420-421 (citations omitted). So there is no reason to believe the CFAA's reference to devices engaged in "foreign commerce or communication" reflects an intent (let alone an unmistakably clear one) to cover foreign conduct.

Accordingly, this Court must determine whether Plaintiff "seeks a (permissible) domestic or (impermissible) foreign application of the provision." *Abitron*, 600 U.S. at 418. The answer depends on whether the "conduct relevant to statute's focus occurred in United States territory." *Id.* (quoting *WesternGeco LLC v. ION Geophysical Corp.*, 138 S. Ct. 2129, 2136 (2018)). It did not. Here, the alleged conduct relevant to the CFAA's focus is unauthorized "access[]" of, or "caus[ing] the transmission of a program" to, a protected computer. 18 U.S.C. § 1030(a)(5)(A)-(C); (*see* ECF 54 ¶¶ 179, 188). Whether viewed as the location from which Defendants allegedly accessed Plaintiff's phone by transmitting an iMessage, or the location of the phone itself when

the alleged access and transmission occurred, such conduct "took place outside the United States." *Kiobel*, 569 U.S. at 124.

Plaintiff does not squarely argue otherwise. She vaguely suggests a broad understanding of where unauthorized computer access occurs. (*See* ECF 70 at 29-30.) But in doing so, she relies on inapposite cases discussing *domestic conduct* aimed at *foreign devices* (which were deemed "protected computers" due to their direct nexus to the United States). *See Ryanair DAC v. Expedia Inc.*, No. C17-1789, 2018 WL 3727599, at *3 (W.D. Wash. Aug. 6, 2018) (U.S. defendant allegedly accessed foreign servers); *In re Apple Inc. Device Performance Litig.*, 347 F. Supp. 3d at 444 (U.S. defendant allegedly accessed foreign phones). Even accepting Plaintiff's statement that unauthorized access "happens simultaneously at the locations of the accessor and the accessed computer" (ECF 70 at 29 (quoting *Ryanair*, 2018 WL 3727599, at *3)), Defendants did not engage in domestic conduct because neither they nor Plaintiff's phone were in the United States at the time of the alleged access. Plaintiff's statement that unauthorized access might also occur at the "limitless possible locations that the transmitted data may pass through" is plainly wrong. (*Id.*) It conflates the location of alleged conduct with the (random) locations of alleged consequences of that conduct—and would lead to the absurd conclusion that every time Congress promulgates internet legislation, it clearly intends to regulate conduct worldwide.

To sum up, the CFAA applies to a defendant who, from the United States, accesses a foreign device with a sufficient connection to the United States, and to a foreign defendant who accesses a domestic device. But the CFAA does not apply to a defendant who, from abroad, allegedly accesses a device located abroad. At a minimum, the CFAA does not cover such wholly foreign allegations with the clarity necessary to overcome the presumption against extraterritoriality.

2. Plaintiff Fails To Plead Sufficient Facts To Support A CFAA Claim

Alternatively, Plaintiff fails to state a CFAA claim because her speculative and conclusory allegations do not plausibly link any Defendant to the alleged unauthorized access. (*See* ECF 63 at 23.) Plaintiff relies largely on the DPA and a Reuters article about DarkMatter. (ECF 70 at 30-31.) But the DPA does not mention Plaintiff, so her suggestion that it implicitly supports her allegations is sheer speculation. As for the *Reuters* piece, "newspaper articles should be credited only to the extent that other factual allegations would be—if they are sufficiently particular and detailed to indicate their reliability. Conclusory allegations of wrongdoing are no more sufficient if they come from a newspaper article than from plaintiff's counsel." *In re Wet Seal, Inc. Sec. Litig*., 518 F. Supp. 2d 1148, 1172 (C.D. Cal. 2007)) (quoting *In re McKesson HBOC Secs. Litig*., 126 F. Supp. 2d 1248, 1272 (N.D. Cal. 2000)). And while "information and belief" allegations may suffice where facts are peculiarly in a defendant's possession, such allegations 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) (quoting Wright & Miller, 5 Fed. Prac. & Proc. Civ. § 1224 (3d ed.)). The Amended Complaint fails that standard because it lacks non-conclusory allegations connecting Defendants to the alleged hack of Plaintiff's phone.

3. The CFAA Claim Fails To Meet The Statutory Requirements

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

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

Plaintiff does not dispute that her alleged physical injury at the hands of Saudi officials was not caused by any alleged CFAA violation. Instead, she argues that "Defendants are incorrect that a causal relationship is required." (ECF 70 at 32.) That is wrong.

The plain language of the CFAA requires causation. Under Section 1030(c)(4)(A)(i), a plaintiff must allege that "the offense *caused* (or, in the case of an attempted offense, would, if completed, have *caused*)," one of the circumstances set forth in subclauses (I)-(V). 18 U.S.C. § 1030(c)(4)(A)(i) (emphasis added). Therefore, the causation requirement applies across those subclauses, including to any alleged "physical injury." *Id.* § 1030(c)(4)(A)(i)(III). Although Plaintiff refers to this as "inapposite language in the criminal provisions of the statute" (ECF 70 at 32), the statute expressly ties its private right of action to the subclauses under Section 1030(c)(4)(A)(i)'s umbrella. *See id.* § 1030(g). Furthermore, the right of action expressly incorporates a causation requirement by extending only to a person who suffers damage or loss "*by reason of a violation of this section*." *Id.* (emphasis added). The fact that the right of action *also* requires that the alleged conduct "involve[] one of the factors" such as physical injury (ECF 70 at 32 (quoting 18 U.S.C. § 1030(g)), does not displace these overarching causation requirements.

The CFAA incorporates an additional *proximate* causation requirement that Plaintiff does not satisfy either. (*See* ECF 63 at 27-29.) Plaintiff does not dispute that the CFAA's civil action 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 thus subject to common law "directness principles," *Bank of Am. Corp. v. City of Miami, Fla.*, 581 U.S. 189, 203 (2017) ("The Court has repeatedly applied directness principles

to statutes with 'common-law foundations.'") (quoting *Anza v. Ideal Steel Supply Corp*., 547 U.S. 451, 457 (2006)), and the "traditional requirement" of proximate cause, *id.* at 201. At least 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*." *Id.* (emphasis added) (citation omitted); *see also Van Buren v. United States*, 141 S. Ct. 1648, 1660 (2021); *Andrews v. Sirius XM Radio Inc*., 932 F.3d 1253, 1263 (9th Cir. 2019); *Fraser v. Mint Mobile, LLC*, No. C 22-00138 WHA, 2022 WL 1240864, at *5 (N.D. Cal. Apr. 27, 2022). Indeed, a common meaning of "involve" is "to relate closely." Involve, *Merriam-Webster Dictionary*, https://www.merriam-webster.com/dictionary/involve (definition 3).

The physical injury Plaintiff alleges—detention and torture by foreign government officials—lacks a close connection to the computer hacking by private actors that the CFAA prohibits. *See Van Buren*, 141 S. Ct. at 1660 (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 § 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.

Plaintiff contends that the alleged intervening actions of Saudi officials to physically harm her were foreseeable (ECF 70 at 33-34), but "foreseeability alone does not ensure the close connection that proximate cause requires." *Bank of Am. Corp.*, 581 U.S. at 202. Nothing in the CFAA suggests that Congress intended to provide a remedy for any "ripples of harm" that flow from a violation. *See id.* (construing the Fair Housing Act not to cover such harms).

"[E]ntertaining suits to recover damages for any foreseeable result of a [statutory] violation," such as a violation of the CFAA, "would risk massive and complex damages litigation." *Id.* (internal quotation marks and citation omitted). Plaintiff's reliance on interpretations of California state law cannot overcome these federal principles. (*See* ECF 70 at 33-34); *see also Fraser*, 2022 WL 1240864, at *2-3 (discussing "[t]he defense of superseding cause" "[u]nder California law"); *Ileto v. Glock Inc.*, 349 F.3d 1191, 1208 (9th Cir. 2003) (same).

Indeed, Plaintiff's authorities undermine, rather than support, her argument that the CFAA reaches injuries caused by third-party use of information obtained through a violation. In *Wofse v. Horn*, the alleged physical injury (anxiety and related emotional harms) stemmed directly from the hacking itself, rather than a third party's use of information procured through a CFAA violation. 523 F. Supp. 3d 122, 140 (D. Mass. 2021). And *Fraser* held that CFAA causation was *lacking* where the theft of cryptocurrency at issue flowed from misuse of unlawfully obtained information. 2022 WL 1240864, at *5. Plaintiff cannot explain why the CFAA does not reach financial loss flowing from third-party use of unlawfully obtained information, but would reach physical injury flowing from the same use.

The statutory text is clear, but Plaintiff also fails to address the Senate Report explaining the addition of "physical injury" to the CFAA—which confirms that Section 1030(c)(4)(A)(i)(III) covers injury that flows directly from a violation rather than from a third party's use of unlawfully obtained information. S. Rep. No. 104-357, at 11 (1996) (Congress added the physical injury provision to address its concern about computer intrusions "causing physical injury to any person"). Because Plaintiff does not allege physical injury flowing directly from Defendants' alleged hacking of her phone, her claim does not come within 18 U.S.C. § 1030(c)(4)(A)(i)(III).

b. The Amended Complaint Fails To Plausibly Allege Loss Of At Least $5,000

Plaintiff does not dispute that "loss" under the CFAA encompasses technological harms and consequential damages that result from interrupted service. *See Van Buren*, 141 S. Ct. at 1660; 18 U.S.C. § 1030(e)(11). Nor does she dispute that her alleged business, economic, and educational losses, loss of a vehicle, impaired ability to carry out human rights work, and lost access to files do not qualify. All other alleged losses are not quantified, and the Amended Complaint does not support an inference that they meet the $5,000 statutory minimum. *See, e.g.*, *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) (dismissing CFAA claim for failure to allege a loss of at least $5,000 where the plaintiff failed to quantify his alleged damages). For example, the Amended Complaint does not allege that Plaintiff incurred any expenses in responding to the alleged hacks, such as paying the "cybersecurity experts" she allegedly "communicat[ed] with." (ECF 70 at 34-35.)

Plaintiff contends that she need not allege payment to the cybersecurity experts she consulted, or anyone else, because the value of the time she spent is sufficient. (ECF 70 at 35.) But the Amended Complaint provides no basis for determining the value of that time. Plaintiff relies on cases where, by contrast, the plaintiffs alleged that paid personnel responded to CFAA violations. *Ticketmaster L.L.C. v. Prestige Ent. West, Inc*., 315 F. Supp. 3d 1147, 1173 (C.D. Cal. 2018) (plaintiff hired third-party consultants, among other costs incurred to respond to alleged violation);[7] *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1066 (9th Cir. 2016) ("It is

[7] *See also* First Am. Compl. ¶ 54, *Ticketmaster*, No. 17-cv-7232 (C.D. Cal.) (ECF 36) ("Ticketmaster recently hired third party consultants to implement additional bot mitigation measures that blocked bots at substantial expense to Ticketmaster (far in excess of $5000).") (cited in *Ticketmaster*, 315 F. Supp. 3d at 1173).

undisputed that Facebook employees spent many hours, totaling more than $5,000 in costs, analyzing, investigating, and responding" to alleged violation); *Svanaco, Inc. v. Brand*, 417 F. Supp. 3d 1042, 1059 (N.D. Ill. 2019) ("Svanaco has offered evidence that, at a minimum, it lost 85 hours of employee time responding to the DDOS attacks, which it values as worth $17,141.").

To excuse the lack of support for her amorphous theory, Plaintiff maintains that caselaw addressing consumer, business, and employment disputes is "of limited application" to her claims. (ECF 70 at 35.)[8] But the CFAA defines loss in financial terms and requires that it exceed $5,000—regardless of the context. 18 U.S.C. § 1030(c)(4)(A)(i)(I). Because Plaintiff does not allege physical injury within the meaning of § 1030(c)(4)(A)(i)(III) or loss of at least $5,000, her CFAA claim should be dismissed.

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

Because the Amended Complaint fails to state a claim under the CFAA, Plaintiff's CFAA conspiracy claim necessary fails. *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*, 185 F.3d 957, 969 (9th Cir. 1999)).

The conspiracy claim also fails under the act of state doctrine, which both sides agree precludes a claim that would require the Court to declare invalid an official act of a foreign sovereign performed within its own territory. (ECF 70 at 36); *see W.S. Kirkpatrick & Co., Inc. v.*

[8] Plaintiff relies on *United Federation of Churches, LLC v. Johnson*, 598 F. Supp. 3d 1084 (W.D. Wash. 2022) as an example of a case where the court recognized a variety of losses. (ECF 70 at 36.) But Plaintiff neglects to mention that the court *dismissed* the plaintiff's CFAA claims for failing to plausibly allege a $5,000 loss. *Id.* at 1094, 1097-1098. While the court held that the plaintiff had plausibly alleged some financial loss due to a loss of membership, the court concluded that the plaintiff failed to allocate the total claimed loss between that membership loss and other losses that she did not "explain how to value." *Id.* at 1097.

Env'l Tectonics Corp., 493 U.S. 400, 404 (1990); *Sea Breeze Salt, Inc. v. Mitsubishi Corp*., 899 F.3d 1064, 1069 (9th Cir. 2018). That is precisely the case here: The Amended Complaint alleges that Defendants conspired with officials of the UAE government in an unlawful manner as part of "the UAE's campaign of persecution against perceived dissidents of itself and Saudi Arabia" (ECF 54 ¶ 140; *see also id.* ¶¶ 65-86, 230-231), and further alleges that Defendants did so from within the UAE (*see id.* ¶¶ 55-86, 218-224). Plaintiff emphasizes that courts sometimes consider allegations implicating foreign states vis-à-vis international law. (ECF 70 at 36.)[9] But her CFAA conspiracy claim alleges a violation of domestic, not international, law. And Plaintiff does not dispute that the policies underlying the act of state doctrine support applying it to that claim. (*See* ECF 63 at 30-31.) Because both the mandatory factors and underlying principles support applying the doctrine, the Court should dismiss Plaintiff's CFAA conspiracy claim.

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

Plaintiff's ATS claim, like her CFAA claim, fails to overcome the presumption against extraterritoriality—and to otherwise state a plausible claim for relief.

1. Plaintiff's ATS Claim Impermissibly Relies On Extraterritorial Conduct

Plaintiff does not allege U.S. conduct relevant to the "focus" of the ATS. *Nestlé USA, Inc. v. Doe*, 141 S. Ct. 1931, 1936 (2021). She does not claim that any of the individual Defendants' conduct occurred in the United States or that any substantial part of their alleged cyber surveillance touched or concerned the United States. Rather, Plaintiff alleges that, while abroad, the individual Defendants conducted cyber surveillance on behalf of a foreign government that targeted persons

[9] The allegations of Plaintiff's ATS claim have no bearing on the applicability of the act of state doctrine to her CFAA conspiracy claim. (*See* ECF 70 at 36.) The conspiracy claim is based on the CFAA, not the ATS. And the Amended Complaint does not assert an ATS claim against DarkMatter.

located in the Middle East, and aided and abetted that foreign government's alleged actions against Plaintiff while she was in the Middle East. (ECF 54 ¶¶ 20, 30-32, 156-168.)

Plaintiff lists the individual Defendants' alleged connections to the United States. (ECF 70 at 38-39.) But each item is inapposite. Plaintiff's communications with U.S. individuals and travel to the United States, events before the alleged hack, and the fortuitous location of Apple's servers and use of U.S. technology do not establish that Defendants engaged in any domestic conduct, let alone conduct relevant to the focus of the ATS.

Plaintiff identifies no case holding that such limited connections "touch and concern the territory of the United States … with sufficient force to displace the presumption against extraterritorial application" and establish jurisdiction under the ATS. *Kiobel*, 569 U.S. at 124-125. In *Doe I v. Cisco Systems, Inc*., "much of the corporation's alleged conduct constituting aiding and abetting occurred in the United States," where Cisco engineers and other personnel allegedly "design[ed] and implement[ed]" the "Golden Shield" Falun Gong surveillance system and provided "long-term customer support," including "'network maintenance,' testing, and training." 73 F.4th 700, 709 (9th Cir. 2023), *petition for panel rehearing and rehearing en banc* filed August 11, 2023; *see also id.* at 737-738 (noting plaintiffs' additional allegations "that Cisco manufactured hardware for the Golden Shield in California; that Cisco employees in California provided ongoing maintenance and support; and that Cisco in California acted with knowledge of the likelihood of the alleged violations of international law and with the purpose of facilitating them"). But an individual defendant's ratification of key decisions while in California was insufficient to overcome the presumption against extraterritorial application of the ATS. *Id.* at 739. Here, the individual Defendants' alleged "key roles" in the "development, maintenance, deployment and

operation" of alleged cybersurveillance (ECF 70 at 42), *all* occurred overseas. (*See* ECF 54 ¶¶ 65-72, 83-110, 133-134, 321.)

Similarly, *Al Shimari v. CACI Premier Technology, Inc.*, 758 F.3d 516 (4th Cir. 2014), involved extensive U.S. conduct. There, employees of a *U.S. corporation* contracted by the *U.S. Department of Interior* (DOI) allegedly tortured prisoners held by the *U.S. military* in a *U.S. facility* in Abu Ghraib, Iraq. *Id.* at 522-523, 528-529; *Al Shimari v. CACI Premier Technology, Inc.*, No. 5181611, 2023 WL 5181611, at *11 (E.D. Va. July 31, 2023). The U.S. connections were extensive: employees were issued security clearances by the U.S. Department of Defense and received training at a facility in the United States; the contractor was paid based on invoices it mailed to DOI (U.S.) accounting offices; the contractor made hiring decisions about the employees in the United States; contractor staff located in the United States monitored the contractor's personnel reporting structure; and managers of the contractor located in the United States allegedly were aware of the misconduct, encouraged it, and attempted to cover it up. 758 F.3d at 523, 528-529; 2023 WL 5181611, at *11-13. 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." 758 F.3d at 528 (quoting *Kiobel*, 569 U.S. at 124). Plaintiffs' other authorities are in the same vein. *See Jane W. v. Thomas*, 560 F. Supp. 3d 855, 877 (E.D. Pa. 2021) (defendant allegedly attacked a compound under the control of a United States agency, resided in the United States, and was deceptive about his role in the attack when he immigrated into the United States); *Mwani v. Bin Laden*, 947 F. Supp. 2d 1, 5 (D.D.C. 2013) (attack on United States embassy and employees with intention of harming the United States and its citizens, as part of a conspiracy to attack the United States). This case is nothing like those.

2. Plaintiff Does Not Allege An Actionable ATS Violation

In any event, Plaintiff does not adequately allege an ATS violation. She alleges that the UAE and Saudi Arabia "persecute and cooperate in the persecution of their respective perceived dissidents" (ECF 54 ¶ 36), albeit in general terms and mostly about third parties not before this Court.[10] But there is no basis for the Court to expand its "narrow" authority to create a cause of action under the ATS—which is limited to violations of 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 (2014))—to extend to the individual Defendants' alleged cyber surveillance.[11] The Ninth Circuit has recognized that "[t]he status of peacetime espionage under international law is a subject of vigorous debate," *Broidy Cap. Mgmt., LLC v. State of Qatar*, 982 F.3d 582, 592 (9th Cir. 2020), *cert. denied*, 141 S. Ct. 2704 (2021), which counsels in favor of caution about opining on the legality of the UAE's activities on its own soil, *see also Kiobel*, 569 U.S. at 116-117 (courts should not encroach upon the discretion exercised by the political branches in matters implicating foreign affairs).[12]

Plaintiff relies on inapposite case law addressing widespread, systematic crimes against humanity. For example, in *Cisco*, a U.S. corporation allegedly aided and abetted a Chinese

[10] The only allegations tying the individual Defendants' alleged cyber surveillance to actual persons concern three third-parties—not Plaintiff. (ECF 54 ¶¶ 83-86.) For example, her allegations about UAE and Saudi Arabia actions concerning women activists and other perceived dissidents address only one alleged instance of third party who was the subject of alleged cyber surveillance being arrested. (*Id.* ¶¶ 34-46, 49, 133-134.) And Plaintiff's allegation that the alleged cyber surveillance program "allowed" operatives to hack into hundreds of iPhones (*id.* ¶¶ 91, 133) does not support a conclusion that the UAE took action against owners of those phones.

[11] Amici themselves acknowledge "that cross-border surveillance is a relatively common practice." (ECF 71 at 7 (internal quotation marks omitted).)

[12] Contrary to Plaintiff (ECF 70 at 34), Defendants rely on *Broidy* with respect to the scope of the ATS—not to assert immunity.

campaign against the Falun Gong that involved persecution of "hundreds of thousands of Falun Gong adherents." 73 F.4th at 712. In *Cisco*, moreover, there were plausible allegations that the defendants knew their actions would lead to "human rights abuses." *See id.* at 734 ("Plaintiffs allege Cisco acted with actual and constructive knowledge of the intended uses of the Golden Shield project, particularly its use in the *douzheng* of Falun Gong, which involved a substantial likelihood of human rights abuses."); *id.* (recounting detailed allegations of Cisco's knowledge, including "Cisco reports" that "referred to 'Strike Hard' campaigns against 'evil cults'"); *see also Jane W.*, 560 F. Supp. 3d at 884-889 (defendant participated in widespread, systematic assaults that were ethnically motivated war crimes); *Sexual Minorities Uganda v. Lively*, 960 F. Supp. 2d 304, 311 (D. Mass. 2013) (defendant allegedly "devised and carried out a program of persecution" targeting the LGBTI community in Uganda); *Wiwa v. Royal Dutch Petroleum Co.*, 626 F. Supp. 2d 377 (S.D.N.Y. 2009) (defendant allegedly aided and abetted attacks of villages, beating, raping, killing, and arresting residents over multiple years); *Kiobel*, 569 U.S. at 113 (describing *Wiwa* allegations on review);[13] *Doe v. Qi*, 349 F. Supp. 2d 1258, 1308 (N.D. Cal. 2004) (discussing "claims alleging genocide and interference with freedom of religion and belief" against the Falun Gong, much like *Cisco*).

This case, by contrast, involves allegations of aiding and abetting UAE cyber-surveillance, not aiding and abetting torture or other crimes against humanity. Plaintiff does not allege that individual Defendants participated in the false arrest or torture she describes, or that they knew such actions would occur. Moreover, Plaintiff's statement that "[t]he Complaint identifies several dissidents who were surveilled by DarkMatter and later arrested" is incorrect. (ECF 70 at 34.) The alleged surveillance of Ahmed Mansoor occurred *after* "the UAE had previously targeted

[13] *Wiwa* went before the Supreme Court as *Kiobel*.

[him] for persecution" (ECF 54 ¶ 83), and she does not allege that the two other individuals mentioned in the Amended Complaint were persecuted (*id.* ¶¶ 85-86). In other words, Plaintiff alleges one incident, not a pattern.

Finally, Plaintiff's remaining cases do not support her allegation of a crime against humanity. She argues that *Mamani v. Berzain*, 654 F.3d 1148 (11th Cir. 2011), indicates that even a small number of victims can establish a crime against humanity. (ECF 70 at 41 n.8.) But *Mamani* held that allegations of 70 killed and approximately 400 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. Nor does *Presbyterian Church of Sudan v. Talisman Energy, Inc*., 226 F.R.D. 456 (S.D.N.Y. 2005), support her assertion that systematic *but not widespread* conduct can constitute a crime against humanity. *See id.* at 457, 464, 481 (applying "requirement that the attack be widespread *and* systematic," in case involving "joint military strategy of ethnic cleansing against the plaintiffs for the purpose of creating a secure buffer zone that facilitated the development and exploitation of oil reserves" that "resulted in *widespread* death, rape, and torture, the enslavement of thousands, vast destruction of property, and the displacement of over 100,000 civilians") (emphases added). Nothing similar is alleged here—and certainly not systematic aiding and abetting of persecution by the *individual Defendants*. Again, Plaintiff is the *only* person she alleges was persecuted following cyber surveillance by Defendants.

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

CONCLUSION

For the foregoing reasons, the Amended Complaint should be dismissed. Plaintiff's second attempt at setting forth a valid theory of personal jurisdiction and plausible claims for relief makes

clear that amendment would be futile. *See Allen v. City of Beverly Hills*, 911 F.2d 367, 373 (9th Cir. 1990). The Court should thus dismiss her claims with prejudice. *See id.*

Respectfully submitted,

Dated: October 30, 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*)
apierce@akingump.com
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