IN THE UNITED STATES DISTRICT COURT

FOR THE 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 **OPINION AND ORDER GRANTING PLAINTIFF'S MOTION FOR LIMITED JURISDICTIONAL DISCOVERY**

Bridget M. Donegan, Boise Matthews, L.L.P., 805 SW Broadway, Suite 1900, Portland, OR 97205. Christopher E. Hart, Andrew B. Lowenstein, and Anthony D. Mirenda. Foley Hoag, L.L.P., 155 Seaport Boulevard, Boston, MA 02210. David Greene and Sabrina S. Cope, Electronic Frontier Foundation, 815 Eddy Street, San Francisco, CA 94109. Carmen K. Cheung, Claret Vargas, and Daniel McLaughlin, Center for Justice and Accountability, 278 Bush Street, Suite 3432, San Francisco, CA 94104. Attorneys for Plaintiff Loujain Hathloul Alhathloul.

Nicholas F. Aldrich, Schwabe, Williamson & Wyatt, P.C., 1211 SW 5th Ave., Suite 1900, Portland, OR 97204. Anthony T. Pierce, Caroline L. Wolverton, and James Tysse, Akin Gump Strauss Hauer & Feld, L.L.P., 2001 K. Street, N.W., Washington, DC 20006. Natasha G. Kohne, Akin Gump Strauss Hauer & Feld, L.L.P., 580 California St., Suite 1500, San Francisco, CA 94104. Attorneys for Defendant DarkMatter Group.

Clifford S. Davidson, Snell & Wilmer, L.L.P., 601 SW 2nd Avenue, Suite 2000, Portland, OR 97204. Attorney for Defendants Marc Baier, Ryan Adams, and Daniel Gericke.

IMMERGUT, District Judge.

Before this Court is Plaintiff Loujain Alhathloul's Motion for Limited Jurisdictional Discovery ("MLJD"), ECF 76. Plaintiff is a human rights activist from Saudi Arabia. According to Plaintiff, Defendants DarkMatter Group, Marc Baier, Ryan Adams, and Daniel Gericke hacked Plaintiff's iPhone, surveilled her movements, and exfiltrated her confidential communications. Plaintiff alleges that these actions led to her arrest by the United Arab Emirates' security services and her rendition to Saudi Arabia, where she was detained and tortured. First Amended Complaint ("FAC"), ECF 54 ¶ 1.

Earlier in this litigation, this Court granted Defendants' motion to dismiss Plaintiff's initial complaint with leave to amend. *See* ECF 44. Thereafter, Plaintiff filed her First Amended Complaint. Defendants then moved to dismiss Plaintiff's First Amended Complaint, contending that this Court lacks personal jurisdiction over all Defendants. *See* Joint Motion to Dismiss ("MTD"), ECF 63. The Motion to Dismiss was fully briefed and taken under advisement on October 30, 2023. ECF 73. A month thereafter, however, the Ninth Circuit issued its decision in *Briskin v. Shopify, Inc.*, 87 F.4th 404 (9th Cir. 2023)—perhaps the first federal appellate opinion in this country addressing "the personal jurisdiction inquiry in cases . . . based on the extraction of . . . data," *id.* at 415.

Following *Briskin*'s publication, Plaintiff now moves for limited jurisdictional discovery to "assess the nature and extent of Defendants' contacts with the" United States. MLJD, ECF 76 at 2. In particular, Plaintiff seeks discovery regarding Defendants' alleged exfiltration of Plaintiff's iPhone data while she was in the United States from November 28 to December 2, 2017. To that end, she requests discovery regarding: (1) the code that comprised the malware used to exfiltrate data from Alhathloul's device; (2) the system architecture of Karma

(Defendant's alleged espionage malware) showing the pathway of interactions between Alhathloul's device and Defendants' servers; (3) the commands sent by Defendants to the malware on Alhathloul's device; and (4) Defendants' awareness of Alhathloul's physical presence in the United States. *Id*. at 6.

In addition, Plaintiff seeks discovery regarding Defendants' contracting with U.S.-based anonymization services and proxy servers, which she claims were instrumental to Defendants' alleged espionage. To that end, she requests discovery regarding: (1) the identity of the companies from which Defendants procured anonymization services and proxy servers; (2) the exact services Defendants procured, including the contract or agreement into which Defendants entered; (3) the role and purpose of these services and proxy servers in furthering hacking activity, including how these anonymization services and proxy servers interacted with other technical features of Karma; and (4) Defendants' reason for choosing these particular anonymization services and proxy servers. *Id.* at 7.

For the reasons below, this Court GRANTS Plaintiff's Motion for Limited Jurisdictional Discovery, ECF 76, but narrows the categories of information Plaintiff may seek. The Parties are ORDERED to propose within fourteen days a two-month limited jurisdictional discovery schedule. This Court RESERVES ruling on Defendants' Motion to Dismiss, ECF 63, pending limited jurisdictional discovery.

LEGAL STANDARDS

District courts have broad discretion in determining whether to permit jurisdictional discovery. *See Boschetto v. Hansing*, 539 F.3d 1011, 1020 (9th Cir. 2008); *see also Data Disc, Inc. v. Sys. Tech. Assocs., Inc.*, 557 F.2d 1280, 1285 n.1 (9th Cir. 1977). "Although a refusal to grant discovery to establish jurisdiction is not an abuse of discretion when it is clear that further

discovery would not demonstrate facts sufficient to constitute a basis for jurisdiction, discovery should be granted when . . . the jurisdictional facts are contested or more facts are needed." *Laub v. U.S. Dep't of Interior*, 342 F.3d 1080, 1093 (9th Cir. 2003) (citation and internal quotation marks omitted); *see also Harris Rutsky & Co. Ins. Servs. v. Bell & Clements Ltd.*, 328 F.3d 1122, 1135 (9th Cir. 2003) (concluding that the district court abused its discretion in denying a motion for jurisdictional discovery and remanding to allow for the opportunity to develop the record).

DISCUSSION

This Court holds that limited jurisdictional discovery is warranted in this matter because key jurisdictional facts are controverted at this procedural juncture. There is a "reasonable probability that the outcome of the factual motion to dismiss" could "be different" following limited jurisdictional discovery concerning (i) Defendants' alleged exfiltration of Plaintiff's iPhone data while she was in the United States from November 28 to December 2, 2017 and (ii) Defendants' contracting with U.S.-based third parties. *Laub*, 342 F.3d at 1093 (internal quotation marks omitted).

In evaluating Plaintiff's motion, this Court holds that jurisdiction here must be analyzed under the framework of purposeful direction. *See Mavrix Photo, Inc. v. Brand Techs., Inc.*, 647 F.3d 1218, 1228 (9th Cir. 2011) ("We have explained that in cases involving tortious conduct, we most often employ a purposeful direction analysis." (citation omitted)). This conclusion follows from Plaintiff's claims. Plaintiff's First Amended Complaint levies three claims against Defendants: Violation of the Computer Fraud and Abuse Act ("CFAA") against all Defendants, Conspiracy to Violate the CFAA against all Defendants, and Crimes Against Humanity under the Alien Tort Statute against the individual Defendants. *See* FAC, ECF 54 ¶¶ 178–234. These "claims sound classically in tort," *Briskin*, 87 F.4th at 412, as the CFAA's cause of action has

been analogized by the Ninth Circuit to "breaking and entering," *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1197–98 (9th Cir. 2022) (citation omitted), and the Alien Tort Statute, by its terms, confers "original jurisdiction of any civil action by an alien for *a tort* only, committed in violation of the law of nations or a treaty of the United States," 28 U.S.C. § 1350 (emphasis added). Accordingly, Plaintiff's claims "are most naturally analyzed under the purposeful direction framework." *Briskin*, 87 F.4th at 412.

Under this rubric, Plaintiff's allegations raise controverted points that are best resolved through limited jurisdictional discovery. To begin with, the Parties contest how Defendants' alleged exfiltration software interacts with Apple's U.S.-based servers. Plaintiff alleges that Defendants' software "necessarily targets and utilizes servers located in the United States" and that it was jurisdictionally significant that Plaintiff was in the United States from November 28 to December 2, 2017 as her phone was being exfiltrated. FAC, ECF 54 ¶¶ 111, 140–55. Defendants counter that the software's interaction with U.S.-based servers is insufficient to establish personal jurisdiction because "Plaintiff would have experienced the same harm wherever else she might have traveled." MTD, ECF 63 at 10 (citation, brackets, and internal quotation marks omitted). But it is not entirely clear based on the current record whether the alleged exfiltration of Plaintiff's iPhone in the United States was made possible, or enhanced, by "some prioritization of the [United States]" or "some differentiation of the [United States] from other locations." *Briskin*, 87 F.4th at 420 (citation omitted); *see Doe v. WebGroup Czech Republic, A.S.*, 89 F.4th 1188, 1199 (9th Cir. 2024) (explaining that a website "differentially target[ing] U.S. visitors . . . constitutes express aiming at the U.S. market"). Limited discovery on how Defendants' software allegedly interacted with, and exfiltrated data from, Plaintiff's

iPhone while she was in the United States can resolve this query with a certainty that, as Defendants recognize, Plaintiff's "information and belief" cannot offer. *See* MTD, ECF 63 at 12.

Further, Plaintiff raises several allegations concerning Defendants' interaction with U.S.-based anonymization services and proxy servers. *See* FAC, ECF 54 ¶¶ 87–110. Through these services and servers, Plaintiff alleges, "Defendants evaded detection and attribution of their attacks, allowing Defendants to persist with the hacking." Plaintiff's Response to MTD, ECF 70 at 7. Defendants contest the relevance of these alleged relationships with third parties, asserting that "there is . . . no allegation (or indication) that DarkMatter worked with companies or technologies because of their alleged links to the United States." MTD, ECF 63 at 11. The Ninth Circuit, however, has instructed that "when considering a defendant's business structure, the role of third parties is important." *Briskin*, 87 F.4th at 420. "Particularly relevant to the defendant's intent to aim activity toward the forum state and its control over that activity is the role of third parties in carrying out the defendant's business operations . . . ." *Id.* (citation omitted); *see WebGroup*, 89 F.4th at 1199 (explaining that the use of a U.S.-based third party's services that "*differentially* favored the United States market was 'good evidence'" of express aiming (citation omitted)). Therefore, it is more than probable that the currently controverted role of these U.S.-based third-party businesses and Defendants' reasons for contracting with them could affect this Court's ultimate ruling on jurisdiction. *See AMA Multimedia, LLC v. Wanat*, 970 F.3d 1201, 1217 (9th Cir. 2020) (R. Nelson, J., concurring) ("If additional jurisdictional discovery is ordered, [the defendant's] contacts with the United States may be shown to be more significant than the current record demonstrates.").

Defendants offer three additional reasons against limited jurisdictional discovery, but none persuades this Court. First, Defendants argue that Plaintiff's motion is untimely. *See*

Defendants' Response to MLJD ("Resp."), ECF 79 at 3. The Ninth Circuit, however, issued its opinion in *Briskin*—again, perhaps the first federal appellate opinion in this country addressing "the personal jurisdiction inquiry in cases . . . based on the extraction of . . . data," 87 F.4th at 415—only after the briefing on Defendants' Motion to Dismiss had been completed. Therefore, in this Court's view, it was not untimely for Plaintiff to seek limited discovery to establish a concrete record in accord with *Briskin*'s reasoning. *See WebGroup*, 89 F.4th at 1204–05 (Lee, J., concurring) ("[I]t would have been prudent for the district court to have ordered very limited jurisdictional discovery here. Such discovery would have tethered the district court's analysis more tightly onto our circuit's personal jurisdiction framework."); *see also Good Job Games Bilism Yazilim Ve Pazarlama A.S. v. SayGames, LLC*, No. 20-16123, 2021 WL 5861279, at *1 (9th Cir. Dec. 10, 2021) (recognizing that "[t]he question of jurisdiction in the Internet age is not well-settled" and reversing and remanding for jurisdictional discovery).

Second, Defendants assert that "under the guise of jurisdictional discovery," Plaintiff's motion is in fact attempting "to prove her case on the merits." Resp., ECF 79 at 5 (citation, brackets, and internal quotation marks omitted). However, "[s]imply because the discovery requested may reveal facts relevant to both jurisdiction and the merits does not preclude that discovery from being jurisdictional in nature." *In re Cathode Ray Tube Antitrust Litig.*, Case No C-07-5944 JST, 2018 WL 4775595, at *4 (N.D. Cal. Aug. 20, 2018). Moreover, this Court will impose two key limits on the jurisdictional discovery here. The discovery shall be limited to facts relevant to the purposeful direction framework outlined in *Briskin*. *See supra* at 4–5. And the discovery shall be limited to information relevant to Defendants' alleged espionage while Plaintiff was in the United States from November 28 to December 2, 2017. *See infra* at 8–9.

Third, Defendants contend that jurisdictional discovery "would circumvent Defendants' due process rights" as foreign residents. Resp., ECF 79 at 6. This concern is reasonable; as the Supreme Court has recognized, however, such concerns can be addressed by the limited scope of discovery and careful judicial supervision of the discovery process. *See Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Ct. for S. Dist. of Iowa*, 482 U.S. 522, 546 (1987) (explaining that "[w]hen it is necessary to seek evidence abroad . . . the district court must supervise pretrial proceedings particularly closely to prevent discovery abuses").

CONCLUSION

This Court GRANTS Plaintiff's Motion for Limited Jurisdictional Discovery, ECF 76, with limiting modifications. Plaintiff will be permitted to seek discovery regarding the following eight categories of information:

> (1) the code that comprised the malware used to exfiltrate data from Alhathloul's device;
>
> (2) the system architecture of Karma (Defendant's alleged espionage malware) showing the pathway of interactions between Alhathloul's device and Defendants' servers, in anticipation of and during Alhathloul's visit to the United States from November 28 to December 2, 2017;
>
> (3) the commands sent by Defendants to the malware on Alhathloul's device, in anticipation of and during Alhathloul's visit to the United States from November 28 to December 2, 2017;
>
> (4) Defendants' awareness of Alhathloul's physical presence in the United States from November 28 to December 2, 2017;
>
> (5) the identity of the companies from which Defendants procured anonymization services and proxy servers with respect to Alhathloul's iPhone;
>
> (6) the exact services Defendants procured, including the contract or agreement into which Defendants entered with respect to Alhathloul's iPhone;

(7) with respect to Alhathloul's iPhone, the role and purpose of these services and proxy servers in furthering hacking activity, including how these anonymization services and proxy servers interacted with other technical features of Karma; and

(8) Defendants' reason for choosing these particular anonymization services and proxy servers.

The Parties are ORDERED to propose within fourteen days a two-month limited jurisdictional discovery schedule. This Court RESERVES ruling on Defendants' Motion to Dismiss, ECF 63, pending limited jurisdictional discovery.

IT IS SO ORDERED.

DATED this 8th day of February, 2024.

/s/ Karin J. Immergut
Karin J. Immergut
United States District Judge