

United States District Court
Northern District of California

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

SARAH ANDERSEN, et al.,
Plaintiffs,
v.
STABILITY AI LTD., et al.,
Defendants.

Case No. [23-cv-00201-WHO](#) (LJC)

**ORDER GRANTING DEFENDANTS’
REQUEST REGARDING
DISCLOSURE TO DR. ZHAO**

Re: Dkt. No. 300

Before the Court is the parties’ joint discovery letter regarding disclosure of highly confidential materials to Plaintiffs’ expert, Dr. Ben Yanbin Zhao. ECF No. 300. Defendants object to Plaintiffs disclosing highly confidential material designated as “ATTORNEYS’ EYES ONLY” or “HIGHLY CONFIDENTIAL – SOURCE CODE” to Dr. Zhao. Plaintiffs wish to be able to disclose highly confidential material to Dr. Zhao, who, they contend is “one of the preeminent researchers in” the field of AI image generation and thus an invaluable expert. *Id.* at 300.

Dr. Zhao is a computer science professor at the University of Chicago who researches generative AI and machine learning. ECF No. 300-1 (Zhao Decl.) ¶¶ 1-2. As part of his academic research, Dr. Zhao leads the Glaze Project, a “research effort that develops technical tools with the explicit goal of protecting human creatives against invasive uses of generative artificial intelligence[.]” *Id.* ¶ 6. These tools include Glaze, “a tool that makes subtle changes to digital artwork to prevent AI models from accurately mimicking an artist’s unique style[.]” and Nightshade, “a tool that alters core image data, causing AI models that train on these images to produce distorted or incorrect outputs for certain prompts[.]” ECF No. 300 at 2. Defendants contend that Dr. Zhao’s tools “sabotage the training of text-to-image models” and object to

1 disclosing their source code and other highly confidential material to someone who they believe
2 could use it “to more effectively harm Defendants’ products and companies.” *Id.* at 5.

3 “A witness who is qualified as an expert by knowledge, skill, experience, training, or
4 education” may provide opinion testimony if their testimony “will help the trier of fact”
5 understand the evidence or “determine a fact in issue[.]” Fed. R. Evid. 702. “In the ordinary
6 course of litigation, a party is owed some degree of deference in retaining and preparing an expert
7 with the relevant industry experience and availability.” *GPNE Corp. v. Apple Inc.*, No. 12-cv-
8 2885, 2014 WL 1027948, at *1 (N.D. Cal. Mar. 13, 2014) (quotations omitted). But that interest
9 “must be balanced against...[the] risk of improper use or disclosure[.]” *Id.* While there is “no
10 bright-line rule for expert disqualification,” courts must balance the “risk of competitive harm
11 arising from disclosure...against the showing made as to the need for the particular expert or
12 consultant to access the confidential information.” *Kane v. Chobani, Inc.*, No. 12-CV-02425,
13 2013 WL 3991107, at *5 (N.D. Cal. Aug. 2, 2013) (quotations omitted); *Tomahawk Mfg., Inc. v.*
14 *Spherical Indus., Inc.*, 344 F.R.D. 468, 473 (D. Nev. 2023). The parties’ Protective Order
15 establishes that the party “opposing disclosure to the Expert shall bear the burden of proving that
16 the risk of harm that the disclosure would entail (under the safeguards proposed) outweighs the
17 Receiving Party’s need to disclose the Protected Material to its Expert.” ECF No. 276 ¶ 7.4. The
18 Court addresses these two factors—the risk of harm that disclosure to Dr. Zhao may cause
19 Defendants and Plaintiffs’ need to disclose highly confidential information to Dr. Zhao—in turn.

20 Defendants argue that disclosing their highly confidential material, including source code
21 and training data, to Dr. Zhao “raises serious competitive concerns” as Dr. Zhao’s research
22 focuses on developing tools that actively undermine their models.¹ ECF No. 300 at 5. Plaintiffs
23 contend that Dr. Zhao is not an “actual competitor” of Defendants because he is an academic
24 researcher whose work is funded by grants and is not competing “for the same dollars from the
25

26 ¹ They also argue that the protective order directly bars Dr. Zhao from being designated as an
27 expert, as it prohibits past or current employees of a “Party or of a Party’s competitor” from
28 service as an expert. ECF No. 276 ¶ 2.7. As the protective order does not define “competitor,”
this does not meaningfully impact the Court’s analysis. The core issue is if disclosure to Dr. Zhao
creates a risk of competitive harm.

1 same target audience” as Defendants, and thus there is little risk of competitive harm. ECF No.
 2 300 at 3 n.1; *Los Angeles Cnty. Med. Ass’n v. Aetna Health of California, Inc.*, No. CV1211020,
 3 2013 WL 12146515, at *3 (C.D. Cal. Apr. 29, 2013) (defining “direct competitors” in the
 4 consumer protection context as “those who vie for the same dollars from the same consumer
 5 group”). They further argue that accessing Defendants’ highly confidential materials “would
 6 provide zero substantive benefit” to Dr. Zhao’s academic research as he could not determine
 7 whether Defendants “detected and removed” Nightshade-protected images or implemented
 8 countermeasures against his tools “through examination of source code or training data.” ECF
 9 No. 300 at 3.

10 The Court disagrees with Plaintiffs’ argument that Dr. Zhao is not a competitor because he
 11 is an academic researcher rather than part of a company that directly competes “for the same
 12 dollars” as Defendants. *Id.* at 3 n.1. His work is “in functional competition with Defendants” as
 13 he develops tools that attack Defendants’ generative AI models. *Id.* at 5; *see Voice Domain*
 14 *Techs., LLC v. Apple*, Civil Action No. 13-40138, 2014 WL 5106413, at *4 (D. Mass. Oct. 8,
 15 2014) (“Even where parties are not traditional competitors in the market place, an individual may
 16 still be deemed a [competitor] where the parties are in an adversarial posture and the individual
 17 receiving the highly confidential information would be especially situated to take position that are
 18 directly harmful and antagonistic to the defendant.”) (citation modified). Dr. Zhao attests that his
 19 tools teach generative AI models to make mistakes: a model trained on enough Glaze- or
 20 Nightshade-modified images might produce an image in the style of Jackson Pollock when
 21 prompted to produce a realistic charcoal portrait or produce an image of a leather purse when
 22 prompted to draw a cow. Zhao Decl. ¶¶ 10-11. As Dr. Zhao researches and creates tools that
 23 make generative AI models such as Defendants’ less reliable, his work impacts “Defendants’
 24 ability to operate in the marketplace.”² ECF No. 300 at 5; *see Tomahawk Manufacturing*, 344
 25 F.R.D. at 471-72 (identifying that “special concerns arise when prospective experts or consultants

26 _____
 27 ² Plaintiffs argue that Dr. Zhao’s tools only undermine Defendants’ models “insofar as Defendants
 28 misappropriate artists’ work” and thus do not pose a cognizable competitive risk. ECF No. 300 at
 3. This argument is premature, as whether or not Defendants’ use of artists’ work “found on the
 web” to train their AI models is misappropriation is the central issue of this case. *Id.* at 5.

1 may themselves be competitive with the disclosing party’s business”).

2 The Court credits Dr. Zhao’s attestation that “development of Glaze and Nightshade is, for
3 all intents and purposes, complete” and that accessing “Defendants’ training data information
4 would not benefit [his] development of Glaze or Nightshade.” Zhao Decl. ¶¶ 12, 17. But Dr.
5 Zhao has not agreed to cease developing other so-called “data-poisoning tools” during the course
6 of this litigation or to cease researching how to make image-generating AI models less effective.
7 *Id.*; ECF No. 300 at 6 n.12. This is, of course, a wholly legitimate choice, but one that implicates
8 Dr. Zhao’s ability to review Defendants’ highly confidential materials in this case. Per Plaintiffs,
9 Dr. Zhao’s focus is on “adversarial machine learning and tools to mitigate harms of generative AI
10 models[.]” ECF No. 302-6 at 2. Akin to *GPNE*, Dr. Zhao has researched and developed tools that
11 work at cross-purposes with Defendants’ models “[i]n the very recent past,” and “there has been
12 no representation or agreement that he will not do so again in the very near future.” 2014 WL
13 1027948, at *2. His research puts him in an “adversarial posture” vis-à-vis Defendants such that
14 “the information to which he would be exposed as an expert in this case could influence his”
15 ongoing and future work “protecting human creatives against invasive uses of generative artificial
16 intelligence[.]” *Voice Domain*, 2014 WL 5106413, at *4; *GPNE*, 2014 WL 1027948, at *2; Zhao
17 Decl. ¶ 6. This is in no way to suggest that Dr. Zhao would intentionally misuse information
18 obtained during this litigation, but instead recognizes that “even if he were to make his best efforts
19 to cabin the information off in his mind,” the highly confidential information may “become
20 intertwined with his other knowledge such that” it may be disclosed “in the course of his future
21 work[.]” *GPNE*, 2014 WL 1027948, at *2; *Symantec Corp. v. Acronis Corp.*, No. 11-5310, 2012
22 WL 3582974, at *2 (N.D. Cal. Aug. 20, 2012).³ The Court accordingly finds that Defendants have
23 demonstrated that disclosing their highly confidential information to Dr. Zhao poses a risk of
24 harm.

25 Given the risk of harm to Defendants, Dr. Zhao must have “unique knowledge within” the
26 field of AI image generation to review Defendants’ materials designated as highly confidential.

27 _____
28 ³ His agreement to not use any confidential information outside of this litigation thus does not
change this analysis. *See* Zhao Decl. ¶ 5.

1 *Symantec*, 2012 WL 3582974, at *2. Defendants recognize that Dr. Zhao is qualified to serve as
2 an expert but argue that he does not have “unique qualifications that other experts could not
3 provide.” ECF No. 303 at 1; *GPNE*, 2014 WL 1027948, at *1. The Court agrees.

4 AI image generation is a relatively new field, and the Court accepts, as Plaintiffs argue,
5 that the pool of “qualified experts in AI image generation not employed by direct competitors” of
6 Defendants is small. ECF No. 300 at 4. But Defendants demonstrate that it is not “such a niche
7 field that there is only one qualified expert.”⁴ ECF No. 303 at 2. Defendants point to numerous
8 academic papers addressing text-to-image generation; they reason that, between the hundreds of
9 authors of these papers, it is not feasible that “Plaintiffs couldn’t find *anyone* with the ability to
10 explain how generative image models behave” aside from Dr. Zhao. ECF No. 303 at 2. To
11 illustrate their point, Defendants note that one of Dr. Zhao’s former students, Dr. Emily Wenger,
12 had recently been disclosed as an expert on AI image generation a parallel generative AI case.
13 ECF No. 303 at 2. (Dr. Wenger has since been designated as an expert in that case, over the
14 defendants’ objections. *In re Google Generative AI Copyright Litigation*, No. 23-cv-03440-EKL,
15 ECF No. 172 at 1-2 (N.D. Cal. July 10, 2025).) That another academic has been designated as an
16 expert regarding the same topic in a similar case strongly supports Defendants’ point that there is
17 more than “one qualified expert” and Dr. Zhao, although qualified, is not uniquely qualified to
18 “help the Court and the jury in understanding how generative image models memorize, output,
19 and infringe copyrighted work.”⁵ ECF Nos. 303 at 2; 302 at 3.

20 The Court accordingly finds that the risk of harm to Defendants outweighs Plaintiffs’ need
21 to disclose Defendants’ information designated as “ATTORNEYS’ EYES ONLY” or “HIGHLY
22 CONFIDENTIAL – SOURCE CODE” to Dr. Zhao. ECF No. 300 at 1; *see GPNE*, 2014 WL

24 ⁴ Plaintiffs’ own briefing does not contradict this. They claim that “Dr. Zhao is not merely one
25 among several qualified experts” but then explain that he is “*one of the preeminent researchers in*
26 *his field*” and there are a “*few independent experts*” of his caliber. ECF No. 302 at 2, 3 (emphasis
added).

27 ⁵ For the avoidance of doubt, the Court takes no position on whether or not it would designate Dr.
Wenger as an expert in this case if Plaintiffs were to retain her or Dr. Wenger were to agree to
serve as an expert. *See* ECF No. 309 at 2. That dispute is not before the Court. The Court
discusses Dr. Wenger only to illustrate that other qualified experts exist. *See GPNE*, 2014 WL
1027948, at *2.

1 1027948, at *2. Defendants' request that any information so designated shall not be disclosed to
2 Dr. Zhao is granted.

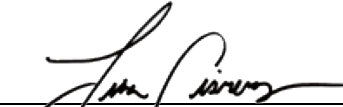
3

4 **IT IS SO ORDERED.**

5 Dated: July 14, 2025

6

7



LISA J. CISNEROS
United States Magistrate Judge

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

United States District Court
Northern District of California