

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

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

SWARMIFY, INC.,
Plaintiff,
v.
CLOUDFLARE, INC.,
Defendant.

No. C 17-06957 WHA

**ORDER ON MOTION
TO STRIKE**

INTRODUCTION

In this action for trade secret misappropriation, defendant moves to strike the latest list of asserted trade secrets that plaintiff disclosed pursuant to Section 2019.210 of the California Code of Civil Procedure. The motion is **GRANTED IN PART** and **DENIED IN PART**.

STATEMENT

The issue is a recurring one, the question of the extent to which a trade secrets plaintiff in a federal action may be permitted to adjust its list of asserted trade secrets after having obtained access to the files of the accused.

This is an action by plaintiff Swarmify, Inc., against defendant Cloudflare, Inc., for trade secret misappropriation and related state law claims. Swarmify fired the opening salvo in this action with a motion for a preliminary injunction. During briefing on that motion, Swarmify filed its original disclosure of six alleged trade secrets pursuant to Section 2019.210 of the California Code of Civil Procedure. The disclosure’s contents and the complaint’s allegations have been described in detail in a prior order dated February 27, which denied Swarmify’s

1 motion for a preliminary injunction based on failure to show likelihood of irreparable harm.
2 Although it did not actually reach the merits, the February 27 order also discussed at length the
3 “overbreadth of Swarmify’s various and ever-shifting descriptions of its supposed trade secrets”
4 and noted that “Swarmify’s attempts to set up its purported trade secrets as elusive moving
5 targets do not bode well for the merits of its claims” (*see* Dkt. No. 88 at 4–6).

6 After the dust settled on its motion for a preliminary injunction, Swarmify filed a new
7 disclosure of five alleged trade secrets under Section 2019.210. Despite the fact that Swarmify
8 had already made quicksand of its asserted trade secrets — a problem explicitly called out in the
9 February 27 order — the new disclosure once again drastically overhauled its descriptions of
10 the technology Cloudflare allegedly misappropriated. Cloudflare now moves to strike both the
11 new disclosure and the deficient portions of Swarmify’s original disclosure, protesting that
12 Swarmify cannot “take a second bite at the apple” after losing at the preliminary injunction
13 stage but obtaining valuable information about Cloudflare’s litigation strategy and defenses
14 (Dkt. No. 101). Swarmify responds that the new disclosure should be allowed because the
15 February 27 order amounted to “an instruction to provide clarification on [Swarmify’s] claimed
16 trade secrets.” If that was not the message of the February 27 order, Swarmify says, it would be
17 “content to stand on its Original Disclosure” (Dkt. No. 107 at 2). Swarmify also insists it has
18 not improperly used discovery to overhaul its Section 2019.210 disclosure and, in the
19 alternative, seeks leave to amend its disclosure yet again (*see id.* at 13).

20 This order follows full briefing and oral argument.

21 ANALYSIS

22 Section 2019.210 provides:

23 In any action alleging the misappropriation of a trade secret
24 under the Uniform Trade Secrets Act . . . before commencing
25 discovery relating to the trade secret, the party alleging the
misappropriation shall identify the trade secret with
reasonable particularity.

26 The parties have offered no analysis or authority to explain whether or how this provision
27 should apply where, as here, discovery has already commenced in a federal action, but it is a
28 point worth clarifying. The plain text of Section 2019.210 does not contemplate this scenario.

1 Our court of appeals has not spoken directly on the issue, but has cited with approval *Universal*
2 *Analytics v. MacNeal-Schwendler Corp.*, 707 F. Supp. 1170, 1177 (C.D. Cal. 1989) (Judge
3 Stephen Victor Wilson), for the proposition that the plaintiff “should describe the subject matter
4 of the trade secret with *sufficient particularity* to separate it from matters of general knowledge
5 in the trade or of special knowledge of those persons skilled in the trade.” *Imax Corp. v.*
6 *Cinema Techs., Inc.*, 152 F.3d 1161, 1164–65 (9th Cir. 1998). *Universal Analytics*, in turn, took
7 that proposition from *Diodes, Inc. v. Franzen*, 260 Cal. App. 2d 244, 253 (1968), the “seminal
8 decision” that became “the genesis of [S]ection 2019.210.” *Brescia v. Angelin*, 172 Cal. App.
9 4th 133, 147 (2009). In other words, while *Imax* did not explicitly discuss Section 2019.210, it
10 applied the core principle codified therein.

11 In doing so, *Imax* affirmed a district court’s decision — after commencement of
12 discovery — to grant summary judgment for the defendant on a trade secret misappropriation
13 claim where the plaintiff had failed to identify its alleged trade secrets with sufficient
14 particularity. *See* 152 F.3d at 1164–68. Consistent with this approach, judges in our district —
15 including the undersigned judge — faced with deficient disclosures under Section 2019.210
16 have routinely entertained defense motions to defeat trade secret misappropriation claims after
17 commencement of discovery, whether styled as a “motion to strike,” “motion for summary
18 judgment,” or something else. *See, e.g., Openwave Messaging, Inc. v. Open-Xchange, Inc.*,
19 2018 WL 692022, at *4 (N.D. Cal. Feb. 2, 2018) (Judge William Orrick) (examining adequacy
20 of Section 2019.210 disclosure on motion for summary judgment); *BladeRoom Grp. Ltd. v.*
21 *Facebook, Inc.*, 2018 WL 514923, at *3–5 (N.D. Cal. Jan. 23, 2018) (Judge Edward Davila
22 (same); *Waymo LLC v. Uber Techs., Inc.*, 2017 WL 5000352, at *7–9 (N.D. Cal. Nov. 2, 2017)
23 (Judge William Alsup) (granting overlapping motions to strike and for summary judgment on
24 trade secret misappropriation claim); *Jobscience, Inc. v. CVPartners, Inc.*, 2014 WL 1724763,
25 at *2–4 (N.D. Cal. May 1, 2014) (Judge William Alsup) (granting motion to strike and
26 dismissing trade secret misappropriation claim) (*Jobscience I*); *Art of Living Found. v. Does*
27 *1–10*, 2012 WL 1565281, at *23 (N.D. Cal. May 1, 2012) (Judge Lucy Koh) (inviting motion
28 for summary judgment on trade secret misappropriation claim).

1 Insofar as controlling law on this subject remains ambiguous, district courts may also
2 exercise discretion in case management to enforce Section 2019.210, and the undersigned judge
3 has in fact done so. *See, e.g., Jobscience, Inc. v. CVPartners, Inc.*, 2014 WL 852477, at *4–5
4 (N.D. Cal. Feb. 28, 2014) (*Jobscience II*). Approaching the issue as one of case management
5 also works well because, technicalities aside, Section 2019.210 ultimately aims to address
6 practical problems that tend to arise in trade secret litigation. *See Advanced Modular*
7 *Sputtering, Inc. v. Superior Court*, 132 Cal. App. 4th 826, 835 (2005) (“[T]he law is flexible
8 enough for the referee or the trial court to achieve a just result depending on the facts, law, and
9 equities of the situation.”). Among other things, it “promotes well-investigated claims and
10 dissuades the filing of meritless trade secret complaints,” “prevents plaintiffs from using the
11 discovery process as a means to obtain the defendant’s trade secrets,” and “enables defendants
12 to form complete and well-reasoned defenses.” *Id.* at 833–34. “Experience has shown that it is
13 easy to allege theft of trade secrets with vagueness, then take discovery into the defendants’
14 files, and then cleverly specify what ever happens to be there as having been trade secrets stolen
15 from plaintiff.” *Jobscience I*, 2014 WL 1724763, at *2.

16 The foregoing practical concerns bear on the instant motion. *First*, Swarmify should not
17 be allowed to drag Cloudflare into court based on meritless arguments, only to reboot its alleged
18 trade secrets lineup and try again when the opening skirmish illuminates glaring flaws in
19 Swarmify’s case. *Second*, Swarmify represents that it has not used information gained in
20 discovery to redefine its alleged trade secrets, and Section 2019.210 draws the line at
21 “discovery.” But even if that representation could be relied upon, redefining alleged trade
22 secrets based on information gained by moving for a preliminary injunction, thereby forcing the
23 accused to disclose the details of its technology and defenses, raises a similar concern of abuse.
24 *Third*, Swarmify’s bait-and-switch tactic prejudices Cloudflare, which invested significant time,
25 effort, and legal strategy in opposing Swarmify’s motion for a preliminary injunction but must
26 now rebuild its defenses to react to Swarmify’s new disclosure, having already shown much of
27 its hand to the opposing side. These concerns all indicate that Swarmify’s new disclosure
28 should not be permitted — at least, not without consequence.

1 On the other hand, the new disclosure as a whole has not become so unmoored from the
2 core technology described in the original disclosure that this action, which remains in its early
3 stages, would become unsalvageable if allowed to proceed. Moreover, another practical
4 advantage unique to post-discovery enforcement of Section 2019.210 has also become
5 particularly germane to our case.

6 Gamesmanship, even if well-disguised at the outset, tends to come into clearer focus as
7 litigation progresses. For example, it becomes easier to pinpoint how vaguely-alleged trade
8 secrets may have functioned as moving targets, and how the plaintiff may have taken advantage
9 of the shifting sands of litigation to evade counterarguments. These developments may cast the
10 unreasonableness of the initial disclosure into sharp relief in light of how the alleged trade
11 secrets evolved over time. In such cases, a plaintiff that merely postpones reckoning with
12 Section 2019.210 early on may eventually find that the consequences of their evasions come
13 home to roost in the form of an adverse ruling on the entire trade secret misappropriation claim.
14 *See, e.g., Waymo*, 2017 WL 5000352, at *7–9. As the February 27 order foreshadowed,
15 Swarmify has already gone quite a ways down this path.

16 After weighing the foregoing factors, this order holds that Swarmify may proceed on its
17 new disclosure if it so chooses. To proceed on the new disclosure, however, Swarmify must
18 follow three conditions. *First*, the new disclosure would be the final definition of Swarmify’s
19 alleged trade secrets for this case. No further amendments would be permitted. Cloudflare,
20 however, would still be able to reference the original disclosure in its arguments — for
21 example, to show the jury the shifting-sands nature of Swarmify’s case. *Second*, Swarmify
22 would pay Cloudflare its reasonable attorney’s fees for defending the motion for a preliminary
23 injunction premised on a defunct list of alleged trade secrets. *Third*, Cloudflare would be
24 entitled to additional expedited discovery, including repeat depositions if necessary, to rebuild
25 its defenses with the new disclosure in mind.

26 By **JUNE 7 AT NOON**, Swarmify shall file and serve a statement electing to either
27 proceed on its new disclosure on the conditions set forth above or instead stand on its earlier
28

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

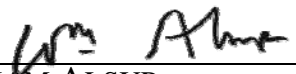
trade secret disclosure. There must be no equivocations or caveats. All appellate rights, of course, shall be reserved as to both sides.

CONCLUSION

For the foregoing reasons, defendant’s motion to strike is **GRANTED IN PART** and **DENIED IN PART**.

IT IS SO ORDERED.

Dated: May 31, 2018.



WILLIAM ALSUP
UNITED STATES DISTRICT JUDGE