

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.,

No. C 17-06957 WHA

Plaintiff,

v.

**ORDER DENYING MOTION  
FOR PRELIMINARY  
INJUNCTION**

CLOUDFLARE, INC.,

Defendant.

**INTRODUCTION**

In this action for trade secret misappropriation and related state law claims, plaintiff moves for a preliminary injunction. The motion is **DENIED**.

**STATEMENT**

Plaintiff Swarmify, Inc., a small start-up based in Melbourne, Florida, formed in 2013 with the sole purpose of creating and bringing to market a method for more reliable and affordable internet video streaming. To that end, according to chief executive officer and co-founder Nathan Barnett, Swarmify spent approximately one million dollars and invested approximately 21 thousand hours in research and development from 2013 to 2015, and “at least an equal amount of time and money on additional improvements and refinements” through 2017 (Dkt. No. 18-11 ¶¶ 2–3). The fruit of those labors became what Swarmify calls its “proprietary method” of video streaming, described “[i]n general” and “without limitation” by Barnett as follows (*id.* ¶¶ 4–5):

1 When a content user (i.e., viewer of a video) requests to view a  
2 video from a website, Swarmify's system looks to two or more  
3 sources from which to retrieve the requested video where it is  
4 stored. These sources will be different servers on a given network,  
5 such as on a content delivery network. The video is broken into  
6 segments, and each segment can be retrieved from a different  
7 source and incrementally loaded to the viewer's computer from  
8 those different sources, depending on parameters detected by the  
9 system. The first segment of video will normally be loaded from  
10 the closest server to the content user in order to stream video at  
11 maximum speeds and eliminate buffering. However, the closest  
12 server will, in most applications, be the most expensive server  
13 from which to source the video segments.

14 This dynamic switching allows for  
15 rapid delivery of video segments when needed to prevent buffering  
16 but, when not needed, allows the content requestor to pull video  
17 from sources that are under-utilized and currently carrying less  
18 traffic, thus providing cost savings to the content provider.

19 Swarmify apparently considers all of the foregoing, "as well as the research and information  
20 used in development [thereof] and the methods used in its implementation, to be its confidential  
21 and proprietary information" (*id.* ¶ 6).

22 On September 11, 2015, Swarmify applied for a patent that would cover "a substantial  
23 portion" of the foregoing technology. That application remains pending and unpublished per  
24 Swarmify's request (*id.* ¶ 8).

25 According to Barnett, Swarmify takes various steps to protect the confidentiality of  
26 information pertaining to its streaming method. It requires employees to sign confidentiality  
27 agreements, enforces company policies that require confidentiality, restricts disclosure of  
28 information to a "need-to-know" basis, uses locked office doors and password-protected  
computer systems, and discloses information to third parties and business partners only as  
necessary and pursuant to nondisclosure agreements (*id.* ¶¶ 10–13).

1 In February 2016, Swarmify made contact with Cloudflare, Inc., a San Francisco-based  
2 corporation that formed in 2009 and uses a network of data centers to offer reverse-proxy and  
3 content delivery services to other companies (*see* Dkt. Nos. 42-4, 42-6 ¶¶ 3–11). As part of  
4 negotiations regarding a possible business deal between them, on April 22, 2016, Swarmify and  
5 Cloudflare entered into a non-disclosure agreement “to protect the confidentiality of certain  
6 confidential information . . . to be disclosed . . . solely for use in evaluating or pursuing a  
7 business relationship between the parties” (Dkt. No. 19-9). In April and May 2016, pursuant to  
8 the non-disclosure agreement, Swarmify disclosed to Cloudflare some confidential information  
9 about its streaming method, including its pending patent application (*see* Dkt. Nos. 19-10–19-  
10 11; *see also* Dkt. No. 18-11 ¶¶ 19–21). Significantly, Swarmify did not disclose any computer  
11 code to Cloudflare (Dkt. No. 42-6 ¶ 18).

12 On May 11, 2016, however, Cloudflare’s head of infrastructure Nitin Rao told Barnett  
13 via email that Cloudflare had decided to “hold off on the Swarmify discussion” for the time  
14 being (Dkt. No. 41-11). On May 31, 2017, Cloudflare extended employment offers to Barnett  
15 (Dkt. No. 42-18) and Chris Fung, the senior developer who apparently engineered Swarmify’s  
16 streaming method (Dkt. Nos. 18-11 ¶ 38, 42-19). More negotiations apparently followed. On  
17 June 12, Barnett offered to sell Swarmify’s assets — including intellectual property and  
18 software — to Cloudflare for \$738,000 (Dkt. No. 18-12). On June 17, Barnett also declined  
19 Cloudflare’s offers of employment for himself and Fung, explaining that “the software and  
20 intellectual property from Swarmify will have to be purchased along with the team” (Dkt. No.  
21 18-13). Significantly, in the same email, Barnett also said, “We presented our proprietary  
22 Swarmify video solution to your team over a year ago . . . . *The software to enable this*  
23 *groundbreaking improvement to video streaming required the prior two years of time in*  
24 *research, development, debug, and production testing” (ibid. (emphasis added)). To repeat,*  
25 Swarmify had not disclosed its software to Cloudflare. Nor has Swarmify argued in this lawsuit  
26 that its alleged trade secrets lie in software (as opposed to, *e.g.*, general concepts and ideas).

27 On June 19, 2017, Cloudflare’s chief executive officer and co-founder Matthew Prince  
28 responded to Barnett’s email and turned down Swarmify’s counteroffer of an asset purchase.

1 “With regard to the Swarmify assets,” Prince wrote, “our analysis leads us to value them as a  
2 liability not an asset. We can’t assign any value to them.” Prince offered to “discuss revising”  
3 the employment offers to Barnett and Fung but otherwise concluded, “If you decide to continue  
4 working on Swarmify, I respect that and wish you the best of luck. Know that if anything  
5 changes in the future, our door is always open” (*ibid.*).

6 According to Rao, Cloudflare then hired Oliver Yu, ostensibly an engineer, to begin  
7 work on its own video streaming service in July 2017. By October 2017, the group working on  
8 the project had expanded to include at least three more engineers. Cloudflare had also “entered  
9 into an agreement with another company concerning specific aspects of video-encoding and  
10 video-playing technology.” According to Rao, Cloudflare has spent hundreds of thousands of  
11 dollars on this project (Dkt. No. 42-6 ¶¶ 19–20).

12 On September 27, 2017, Cloudflare marked the launch of its own streaming service with  
13 two blog articles on its public website. *First*, Prince posted “Introducing Cloudflare Stream:  
14 Fixing the Streaming Video Market,” which broadly described some technological and business  
15 challenges to video streaming and Cloudflare’s solutions to those challenges (Dkt. No. 18-17).  
16 *Second*, Yu posted “How Cloudflare Streams,” which described Cloudflare’s solution in more  
17 technical detail (Dkt. No. 18-18). In relevant part, Yu’s article explained:

18 [W]e use a technology called adaptive streaming in which the  
19 server offers multiple bitrate streams and the client switches  
20 between them based on the current network connectivity. To  
21 accomplish this, the video is chunked, and the client can switch  
22 between profiles in between the video chunks by downloading the  
23 following chunk from a different bitrate stream.

24 \* \* \*

25 [Cloudflare delivers video] by

26 [REDACTED]  
27 [REDACTED]  
28 [REDACTED] The final result is that the first segment is fast,  
with low cost subsequent segments.

1 The latter paragraph, according to Barnett, describes “precisely the method by which  
2 Swarmify streams video” (Dkt. No. 18-11 ¶ 42). Swarmify also generally accuses both Prince  
3 and Yu’s articles of disclosing Swarmify’s streaming method (*see, e.g.*, Dkt. No. 18-4 at 14).  
4 Based on those articles, Swarmify filed this action in December 2017. The complaint asserts  
5 claims for trade secret misappropriation under both the federal Defend Trade Secrets Act and  
6 the California Uniform Trade Secrets Act, breach of contract, breach of the implied covenant of  
7 good faith and fair dealing, unjust enrichment, fraud, accounting, and unfair competition in  
8 violation of Section 17200 of the California Business and Professions Code (Dkt. No. 1).

9 Swarmify then filed a motion for a preliminary injunction (Dkt. No. 19). *After*  
10 Cloudflare’s opposition but *before* Swarmify’s reply, Swarmify filed a disclosure of six alleged  
11 trade secrets pursuant to Section 2019.210 of the California Code of Civil Procedure (Dkt. No.  
12 46-3). According to that disclosure, Swarmify’s first alleged trade secret claims a “method for  
13 video streaming” including “*at least*” the “dynamic switching” method set forth in Barnett’s  
14 declaration (emphasis added). The disclosure reinvents Barnett’s description with some notable  
15 differences. For example, the disclosure calls for the first video segment to load from the  
16 “fastest” server instead of the “closest” server. The disclosure also adds:

17 [REDACTED]  
18 [REDACTED]  
19 [REDACTED]  
20 [REDACTED]

21 Swarmify describes its pending patent application as just “one potential manifestation” of its  
22 first alleged trade secret (*id.* at 1–2).

23 To call Swarmify’s disclosure overbroad would be an understatement. In addition to the  
24 first alleged trade secret described above, the five remaining alleged trade secrets, reproduced in  
25 full here, claim (*id.* at 2–3):

- 26 2. The research and information used to develop the  
27 Technology, including aggregation of publicly-available  
28 information or knowledge on prior methods of video streaming.
- 3. The methods for implementing the Technology.

1                   4.       The fact that the Technology is fully functional and  
2 is commercially viable, including market applications, costs, and  
3 benefits. This includes the application and market information that  
4 Swarmify shared with Cloudflare in Exhibit I to the Declaration of  
5 Nathan Barnett in Support of Swarmify’s Motion for Preliminary  
6 Injunction.

7                   5.       Internal data provided to Cloudflare which provides  
8 indications of the costs, transfer used for the various delivery  
9 endpoints, and calculations providing a “blended” cost.

10                  6.       Vendors, and agreements with those vendors, along  
11 with specific pricing, cost, limitations, and usage.

12                  This disclosure, which purports to lay wholesale claim to such nebulous, sweeping  
13 categories as “research and information,” “methods for implementing,” and “vendors,” does not  
14 even come close to identifying plausible trade secrets with “reasonable particularity” as  
15 required by Section 2019.210. Put simply, it is a blatant abuse of the system. The overbreadth  
16 of Swarmify’s various and ever-shifting descriptions of its supposed trade secrets — just a few  
17 examples of which have been reproduced herein — is also further compounded by Swarmify’s  
18 steadfast refusal to pin down in argument the specific nature of the information it claims to own.  
19 Throughout briefing and during the hearing on this motion, Swarmify’s counsel has toggled  
20 between claiming broad, sweeping *concepts* about streaming in general to counter arguments  
21 that Cloudflare never used the supposed trade secrets and claiming narrow, specific  
22 *implementations* of a particular streaming method to dodge arguments that the supposed trade  
23 secrets do not qualify as such because they remain generally known in the field. As explained  
24 below, this order does not reach the merits of Swarmify’s trade secret misappropriation claims  
25 because an even more glaring problem precludes preliminary relief. It nevertheless bears  
26 mentioning that Swarmify’s attempts to set up its purported trade secrets as elusive moving  
27 targets do not bode well for the merits of its claims.

28                  While Swarmify’s motion remained pending, the undersigned judge also required both  
sides to agree to a trial date, having learned the hard way that whichever side prevails on a  
motion for a preliminary injunction usually tries to drag out proceedings thereafter whereas the  
losing side wants a trial as soon as possible (*see* Dkt. No. 58). In response, both sides agreed to

1 proceed to trial on November 13, 2018, which agreement has been codified in the case  
2 management order (Dkt. Nos. 65 at 2, 68). This order follows full briefing and oral argument.

### 3 ANALYSIS

4 To obtain a preliminary injunction, Swarmify must establish that it is likely to succeed  
5 on the merits, that it is likely to suffer irreparable harm in the absence of preliminary relief, that  
6 the balance of equities tips in its favor, and that an injunction is in the public interest. *Winter v.*  
7 *Natural Resources Defense Council, Inc.*, 555 U.S. 7, 20 (2008). In our circuit, “serious  
8 questions going to the merits” and a balance of hardships that tips sharply in Swarmify’s favor  
9 can support issuance of a preliminary injunction so long as Swarmify also shows a likelihood of  
10 irreparable injury and that the injunction is in the public interest. *Alliance for the Wild Rockies*  
11 *v. Cottrell*, 632 F.3d 1127, 1134–35 (9th Cir. 2011).

12 Swarmify relies only on its trade secret misappropriation and breach of contract claims  
13 as the basis for this motion and does not distinguish between those claims for purposes of  
14 asserting likelihood of irreparable harm. Even assuming that some protectible trade secret lurks  
15 within Swarmify’s overbroad and shape-shifting descriptions of its technology, this order  
16 concludes Swarmify has not shown any likelihood of irreparable harm with respect to either its  
17 trade secret misappropriation or breach of contract claims.

18 Swarmify asserts in conclusory fashion that Cloudflare’s alleged misappropriation “will  
19 deprive Swarmify of the years of research and millions of dollars spent developing the  
20 Technology, will allow competitors to cheaply enter the market to Swarmify’s detriment, will  
21 prevent Swarmify from effectively marketing its own innovative Technology to untold numbers  
22 of potential customers, and will continue to prevent Swarmify from attracting investors for its  
23 proprietary streaming solution.” Swarmify also asserts it “will suffer injury to its reputation and  
24 goodwill among actual and potential customers, and among investors, as the premier provider of  
25 such video streaming services” (Dkt. No. 18-4 at 22–23). But the only record evidence  
26 Swarmify cites for its claims of “irreparable harm” comes from two paragraphs of Barnett’s  
27 declaration, which state in similarly conclusory terms (Dkt. No. 18-11 at 11):

28 43. Cloudflare’s actions have caused Swarmify to lose  
market share in the video streaming space — in fact, Swarmify

1 should have been the only company in the market to offer the  
2 solution embodied by its Technology if not for Cloudflare’s  
misappropriation.

3 44. In addition, Swarmify has lost the potential to  
4 attract investors in its innovative, one-of-a-kind solution after  
5 those investors learned that Cloudflare is now doing the same  
6 thing. A true and correct copy of an email from one such investor,  
dated September 29, 2017, is attached as Exhibit L.

6 The sole *factual* component in the foregoing explanation, Exhibit L, fails to support  
7 Barnett’s insinuation that Swarmify lost or will lose investors as a result of Cloudflare’s alleged  
8 misappropriation. That email, from Brian Ascher of Venrock, states, “Your video acceleration  
9 technology sounds awesome, but competing against Cloudflare *and all of the other video*  
10 *incumbents* is a challenging proposition, *especially when the Bigs (YouTube, Netflix, Amazon,*  
11 *Apple, Alibaba, etc[.]) all build their streaming in-house*. Every market can ultimately be  
12 disrupted, but I think we’d need to see more evidence before we could jump in alongside you”  
13 (Dkt. No. 19-20 (emphasis added)). In other words, Venrock declined to invest in Swarmify  
14 because of heavy competition in the video streaming market *in general*, not because any one  
15 competitor duplicated Swarmify’s *specific* streaming method.

16 With the Ascher email excised, Swarmify’s argument about irreparable harm finds itself  
17 devoid of even a glimmer of factual support. Swarmify’s argument essentially boils down to its  
18 insistence that Cloudflare supplanted its commercial market because “Swarmify should be the  
19 only company able to market the Technology” and “any customer buying video streaming  
20 services from Cloudflare is, by definition, not buying them from Swarmify” (Dkt. No. 18-4 at  
21 22–23). In other words, Swarmify is not concerned with the use or disclosure of its alleged  
22 trade secrets by other companies *per se*; its complaint is merely that it, not Cloudflare, should  
23 be the one profiting from this technology.

24 But this is textbook *reparable* harm.

25 If Swarmify prevails on the merits and proves that Cloudflare misappropriated its trade  
26 secrets, Swarmify can be compensated with damages calculated based on Cloudflare’s unjust  
27 enrichment from its use and disclosure of Swarmify’s streaming method. Whatever profit  
28 Cloudflare manages to generate from this technology in the meantime would be fair game for an



1 eventual damages award. Put differently, every dollar of profit Cloudflare makes will be for  
2 Swarmify's account *if* Swarmify's claims hold true.

3 In its reply brief, Swarmify claims for the first time that video streaming is a "young"  
4 industry and that Swarmify's chances of legitimately competing in this industry would be  
5 irrevocably destroyed in the absence of preliminary relief. This argument has no basis in fact or  
6 law. Unsurprisingly, Swarmify cites no record evidence for the proposition that *video*  
7 *streaming in general* is a "young" industry, much less a "nascent" one.

8 Indeed, even a cursory review of the record shows the exact opposite. To give just one  
9 nonexhaustive example, Ascher's email dated September 29, 2017 — the sole item of *factual*  
10 evidence buried in Swarmify's conclusory arguments about irreparable harm — describes  
11 abundant competition in the established video streaming industry that Swarmify was trying to  
12 "disrupt" (Dkt. No. 19-20).

13 In its reply brief, Swarmify quotes selective snippets from the undersigned judge's  
14 provisional relief order in *Waymo LLC v. Uber Technologies, Inc.*, No. C 17-00939, 2017 WL  
15 2123560 (N.D. Cal. May 11, 2017), suggesting an analogy between that case and this one (Dkt.  
16 No. 47-4 at 15).

17 *Waymo* featured alleged trade secrets relating to self-driving car technology. Self-  
18 driving cars represented an unquestionably nascent market. No would-be competitor —  
19 including the parties to that litigation — had managed to actually commercialize that  
20 technology. Damages from the loss of a competitive position in that market would likely have  
21 been impossible to quantify. 2017 WL 2123560, at \*11. Not so here, especially since the  
22 gravamen of Swarmify's complaint remains focused on Cloudflare's *actual* commercialization  
23 of its streaming method. Moreover, in *Waymo* the potential ongoing misuse of the alleged trade  
24 secrets, as both sides continued to develop their respective technologies, might have been  
25 "virtually untraceable." *Id.* at \*10. Here, in contrast, Cloudflare allegedly published two blog  
26 articles detailing its successful implementation and commercialization of the alleged trade  
27 secrets. These facts hardly precipitate the kind of ongoing, elusive misappropriation threatened  
28 in *Waymo*. Finally, *Waymo* involved a key player asserting his Fifth Amendment privilege, as

1 well as other “relentless assertions of privilege” that shrouded relevant events in secrecy such  
2 that it would have been exceptionally difficult to identify and enjoin any specific parts of the  
3 defendants’ technology that used the plaintiff’s alleged trade secrets. *Id.* at \*11. The instant  
4 case presents no such complications, especially since Swarmify’s sweeping disclosure of  
5 alleged trade secrets makes clear that this lawsuit targets Cloudflare’s entire streaming service,  
6 not some subtle part thereof that would be difficult to extricate from the whole.

7 In short, Swarmify’s comparison of this case to *Waymo* collapses under even superficial  
8 scrutiny. The undersigned judge lived through *Waymo*. He knew *Waymo*. This case is not  
9 *Waymo*.

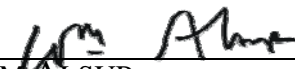
10 Swarmify’s failure to show a likelihood of irreparable harm is a showstopper. *See*  
11 *Winter*, 555 U.S. at 20. This order therefore does not reach the other three *Winter* factors, nor  
12 does it consider the parties’ additional arguments thereunder.

13 **CONCLUSION**

14 For the foregoing reasons, plaintiff’s motion for a preliminary injunction is **DENIED**.  
15 Except to the extent acknowledged herein, defendant’s objection to plaintiff’s reply brief is  
16 **OVERRULED AS MOOT**.

17  
18 **IT IS SO ORDERED.**

19  
20 Dated: February 27, 2018.

21   
22 \_\_\_\_\_  
23 WILLIAM ALSUP  
24 UNITED STATES DISTRICT JUDGE  
25  
26  
27  
28