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 DENYING MOTION FOR PRELIMINARY INJUNCTION**

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):

> When a content user (i.e., viewer of a video) requests to view a video from a website, Swarmify's system looks to two or more sources from which to retrieve the requested video where it is stored. These sources will be different servers on a given network, such as on a content delivery network. The video is broken into segments, and each segment can be retrieved from a different source and incrementally loaded to the viewer's computer from those different sources, depending on parameters detected by the system. The first segment of video will normally be loaded from the closest server to the content user in order to stream video at maximum speeds and eliminate buffering. However, the closest server will, in most applications, be the most expensive server from which to source the video segments. [redacted] This dynamic switching allows for rapid delivery of video segments when needed to prevent buffering but, when not needed, allows the content requestor to pull video from sources that are under-utilized and currently carrying less traffic, thus providing cost savings to the content provider.

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

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 That application remains pending and unpublished per Swarmify's request (*id.* ¶ 8).

According to Barnett, Swarmify takes various steps to protect the confidentiality of information pertaining to its streaming method. It requires employees to sign confidentiality agreements, enforces company policies that require confidentiality, restricts disclosure of 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).

United States District Court
For the Northern District of California

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

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

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

United States District Court
For the Northern District of California

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

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

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

> [W]e use a technology called adaptive streaming in which the server offers multiple bitrate streams and the client switches between them based on the current network connectivity. To accomplish this, the video is chunked, and the client can switch between profiles in between the video chunks by downloading the following chunk from a different bitrate stream.
>
> *　　　　*　　　　*
>
> [Cloudflare delivers video] by [redacted] The final result is that the first segment is fast, with low cost subsequent segments.

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

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

> [redacted]

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

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

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

> 4. The fact that the Technology is fully functional and is commercially viable, including market applications, costs, and benefits. This includes the application and market information that Swarmify shared with Cloudflare in Exhibit I to the Declaration of Nathan Barnett in Support of Swarmify's Motion for Preliminary Injunction.
>
> 5. Internal data provided to Cloudflare which provides indications of the costs, transfer used for the various delivery endpoints, and calculations providing a "blended" cost.
>
> 6. Vendors, and agreements with those vendors, along with specific pricing, cost, limitations, and usage.

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

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

ANALYSIS

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

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

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

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

> should have been the only company in the market to offer the solution embodied by its Technology if not for Cloudflare's misappropriation.
>
> 44. In addition, Swarmify has lost the potential to attract investors in its innovative, one-of-a-kind solution after those investors learned that Cloudflare is now doing the same thing. A true and correct copy of an email from one such investor, dated September 29, 2017, is attached as Exhibit L.

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

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

But this is textbook *reparable* harm.

If Swarmify prevails on the merits and proves that Cloudflare misappropriated its trade secrets, Swarmify can be compensated with damages calculated based on Cloudflare's unjust enrichment from its use and disclosure of Swarmify's streaming method. Whatever profit Cloudflare manages to generate from this technology in the meantime would be fair game for an eventual damages award. Put differently, every dollar of profit Cloudflare makes will be for Swarmify's account *if* Swarmify's claims hold true.

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

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

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

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

United States District Court
For the Northern District of California

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

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

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

CONCLUSION

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

IT IS SO ORDERED.

Dated: February 27, 2018.

WILLIAM ALSUP
UNITED STATES DISTRICT JUDGE