

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

FACEBOOK, INC.,
Plaintiff,
v.

BRANDTOTAL LTD., et al.,
Defendants.

Case No. 20-cv-07182-JCS

**ORDER REGARDING MOTION FOR
TEMPORARY RESTRAINING ORDER**

Provisionally Filed Under Seal

Re: Dkt. No. 27

I. INTRODUCTION

Plaintiff Facebook, Inc. brings this action asserting breach of contract, violation of the Computer Fraud and Abuse Act (“CFAA”), and other claims against Defendants BrandTotal Ltd. and Unimania, Inc. (collectively, “BrandTotal”¹) based on BrandTotal’s collection and marketing of data from Facebook’s websites—specifically, its eponymous social network (hereinafter the “Facebook Network,” in order to distinguish that product from the corporate entity) and Instagram. BrandTotal asserts counterclaims based on Facebook blocking its access to those products, and now moves for a temporary restraining order (“TRO”). The Court held a hearing on October 26, 2020.

BrandTotal has shown serious issues going to the merits of its counterclaims, which implicate difficult questions of balancing—among other considerations—Facebook’s interests in limiting access to its networks, BrandTotal’s interests in maintaining its business, the public interest in competition, and individual users’ potentially conflicting interests in both the privacy of their data and choosing how to share that data. Nevertheless, for the reasons discussed below, the

¹ Unimania, Inc. is a software development subsidiary of BrandTotal Ltd. The parties have identified no relevant distinction between those two entities for the purpose of present motion.

Court DENIES BrandTotal’s motion.²

II. BACKGROUND

A. The Parties’ Allegations and Claims

The following subsections summarize the parties’ factual allegations as context for their respective claims and positions. Nothing in these subsections should be construed as resolving any disputed issue of fact, or as addressing whether any allegation has evidentiary support in the current record. The evidentiary record is addressed in the context of the Court’s analysis.

1. Facebook’s Allegations and Claims

Facebook is a social networking company with billions of individual users across multiple products, including the Facebook Network and the Instagram social network.³ *See* Compl. (dkt. 1) ¶ 13. All users of the Facebook Network agree to contractual terms including that users will not do anything that would “impair the proper working or appearance” of Facebook’s products, will not access or collect data from Facebook’s products “using automated means” without Facebook’s permission, and will not attempt to access data that the particular user lacks permission to access. *Id.* ¶¶ 21, 24, 26. All Instagram users similarly agree not to do “anything to interfere with or impair the intended operation” of Instagram, not to “collect[] information in an automated way without [Facebook’s] express permission,” not to access information “in unauthorized ways,” and not to violate anyone else’s rights, including intellectual property rights. *Id.* ¶¶ 22, 25, 27. Users of both networks agree not to do anything unlawful, misleading, or fraudulent, or to facilitate such activity. *Id.* ¶ 23. According to Facebook, BrandTotal agreed to these terms when it created accounts on the Facebook Network and Instagram. *See id.* ¶¶ 35–39.

Facebook employs various measures to prevent “scraping”—bulk automated collection—of content from its products, including monitoring usage patterns, using “CAPTCHA” tests to determine whether users are human as opposed to automated programs, and disabling accounts

² The parties have consented to the jurisdiction of the undersigned magistrate judge for all purposes pursuant to 28 U.S.C. § 636(c).

³ This case concerns only the Facebook and Instagram social networks. References herein to Facebook’s products or social networks therefore refer to those two networks, and not to any other networks or products that Facebook, Inc. offers.

that violate its rules. *Id.* ¶ 29.

BrandTotal offered programs called UpVoice and Ads Feed that users could install as extensions for the Google Chrome internet browser, which Facebook alleges worked as follows:

Once installed by the users . . . [BrandTotal] used the users’ browsers as a proxy to access Facebook computers, without Facebook’s authorization, meanwhile pretending to be a legitimate Facebook or Instagram user. The malicious extensions contained JavaScript files designed to web scrape the user’s profile information, user advertisement interest information, and advertisements and advertising metrics from ads appearing on a user’s account, while the user visited the Facebook or Instagram websites. The data scraped by [BrandTotal] included both public and non-publicly viewable data about the users.

[BrandTotal’s] malicious extensions were designed to web scrape Facebook and Instagram user profile information, regardless of the account’s privacy settings. The malicious extensions were programmed to send unauthorized, automated commands to Facebook and Instagram servers purporting to originate from the user (instead of [BrandTotal]), web scrape the information, and send the scraped data to the user’s computer, and then to servers that [BrandTotal] controlled.

Id. ¶¶ 45–46. Facebook alleges that BrandTotal collected information including “the user’s ID, gender, date of birth, relationship status, and location information,” users’ “Ad Preferences” information that Facebook used to determine what ads to show them, and—with respect to advertisements that users viewed while using the extension—“information about the advertiser, the image and text of the advertisement, and user interaction and reaction metrics (e.g., number of views, comments, likes) associated with an advertisement.” *Id.* ¶ 54. According to Facebook, the UpVoice and Ads Feed extensions used nearly identical code and functioned materially the same way. *See id.* ¶ 57.

Facebook provides a searchable public library of all advertisements published on its networks, which includes data such as the “Page” responsible for running the ad, the geographic region it is directed to, and the number of users that viewed the ad on a particular day. *See id.* ¶¶ 17–19. Facebook’s public library does not include demographic information about users that viewed a particular ad, or information regarding how users interacted with an ad (e.g., “likes” and comments). *Id.* ¶ 20.

BrandTotal induced users to install these browser extensions by offering gift cards as

1 payment for UpVoice users, by allowing Ads Feed users to review lists of ads they had seen in the
2 last ninety days so that users could return to ads that interested them, and by telling users that they
3 would serve as “panelists” to influence corporate marketing decisions. *Id.* ¶¶ 43–44, 49, 56.
4 BrandTotal analyzed and sold the data that it obtained from users to corporate clients. *Id.* ¶ 37.
5 BrandTotal used different trade names for its browser extensions (which gathered data) and its
6 marketing intelligence product (which incorporated that data), and advertised its products to both
7 potential individual users (who might install the browser extensions and provide data) and
8 potential corporate clients (who might purchase data) on the Facebook Network. *Id.* ¶¶ 39–40, 42,
9 47.

10 According to Facebook, BrandTotal made misleading representations to users of its
11 browser extensions, both by including the Facebook Network in a list of “participating sites” when
12 Facebook had not agreed to work with BrandTotal or authorized it to access Facebook’s data, and
13 by failing to include Instagram in the list of “participating sites” even though the browser
14 extension scraped data from Instagram. *Id.* ¶ 50.

15 On September 30, 2020, Facebook disabled BrandTotal’s accounts on Instagram and the
16 Facebook Network and instated other technological measures to block BrandTotal’s access to
17 Facebook’s products. *Id.* ¶ 58. On October 1, 2020, Facebook filed a civil action against
18 BrandTotal in California state court alleging that the browser extensions breached Facebook’s
19 terms of service. *Id.* ¶ 59.⁴ Later that day, Google removed the browser extensions from its
20 Chrome Web Store, which disabled their functionality. *Id.* ¶ 60. On October 3, 2020,
21 BrandTotal’s chief product officer created accounts on Instagram and the Facebook Network using
22 false names. *Id.* ¶ 61. On October 12, 2020, BrandTotal introduced a new UpVoice browser
23 extension on the Chrome Web Store, listing the developer of the extension as “UpVoice Team.”
24 *Id.* ¶ 62. According to Facebook, the new UpVoice extension—like its predecessors—collected
25 data when users accessed the Facebook Network and returned that data to BrandTotal, including
26

27 ⁴ Facebook voluntarily dismissed its state court action before bringing the present action in this
28 Court, one day before BrandTotal had intended to seek a TRO in state court. Telscher Decl. ¶¶ 6–
8.

data that was, “in some cases, not even viewed by the user.” *Id.* Around thirty users installed this new extension. *Id.*

Facebook asserts the following claims: (1) breach of contract, based on the Facebook Network and Instagram terms of service, *id.* ¶¶ 67–73; (2) unjust enrichment, *id.* ¶¶ 74–80; (3) unauthorized access in violation of the CFAA, *id.* ¶¶ 81–86; (4) unauthorized access in violation of California Penal Code § 502, *id.* ¶¶ 87–95; (5) interference with contractual relations by inducing Facebook’s users to share their login credentials with BrandTotal, in violation of Facebook’s terms of service, *id.* ¶¶ 96–102; and (6) unlawful, unfair, or fraudulent business practices in violation of California’s Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 (the “UCL”), Compl. ¶¶ 103–10. Facebook seeks both injunctive and compensatory relief. *See id.* at 21–22, ¶¶ (a)–(h) (Prayer for Relief).

2. BrandTotal’s Allegations and Claims

BrandTotal is an advertising consulting company that offers its clients analysis of the clients’ own advertising and their competitor’s advertising on social media, including Instagram and the Facebook Network. Counterclaim (dkt. 23) ¶ 8.⁵ BrandTotal alleges that it collects information only after receiving “informed consent and deliberate opt-in” from its users, which users grant in exchange for gift cards. *Id.* ¶ 10. BrandTotal’s users must “confirm they have read the privacy policy which details the demographic and advertising . . . information BrandTotal collects” before they install the UpVoice browser extension. *Id.* ¶ 11.

According to BrandTotal, the UpVoice extension “allows BrandTotal to collect data the user either owns or has a right to access and certain public information about the websites the user visits,” including “the ads they see and interact with on social media sites like Facebook, as they browse as usual on those sites,” and “deidentified information about the user by using hashed values for the user’s device and user IDs.” *Id.* ¶¶ 13–14, 16.

BrandTotal does not collect the user’s names or email addresses, although the user provides that when they sign up. BrandTotal does

⁵ BrandTotal’s Answer and Counterclaim is filed as a single docket entry. Citations herein to the “Counterclaim” refer to paragraphs in the portion of that document so captioned, which begins on page 14.

not keep or compile participants’ private postings, photos, or web history, nor does BrandTotal mine “friend” information, or otherwise take data not expressly authorized. Rather, the information collected relates to who is seeing what advertisement, where and at what times.

Id. ¶ 17. BrandTotal anonymizes the information it collects and provides aggregated data, broken out by demographic information (“age, gender, high level location, marital status, interests”) to its clients. *Id.* ¶ 18.

BrandTotal acknowledges the provision in Facebook’s terms of service prohibiting data collection by automated means without Facebook’s permission, but implies that Facebook’s claimed ability “to pick and choose who . . . will be allowed to access the information” conflicts with other provisions of the terms of service “acknowledg[ing] that users own the rights in their own information.” *Id.* ¶ 21. BrandTotal also alleges that Facebook itself aggregates and sells user data as part of its own advertising consulting service. *Id.* ¶ 22.

According to BrandTotal, Facebook’s actions to cut off BrandTotal’s access to Facebook products and block BrandTotal’s browser extensions from appearing in Google’s Chrome Web Store prevent BrandTotal from compiling advertising analytics for its customers, prevent BrandTotal’s users from logging in “to collect any rewards they have earned,” and prevent BrandTotal from recruiting new participants. *Id.* ¶ 28. BrandTotal customers, including “reputable large companies,” are questioning their relationship, prospective customers that were in negotiations are walking away, and BrandTotal cannot secure receivables, lending, or venture capital investment while it lacks access to Facebook’s networks. *Id.* ¶¶ 29–30. As a result, BrandTotal is “in jeopardy of being insolvent.” *Id.* 31.

BrandTotal asserts the following counterclaims: (1) intentional interference with contract, based on contracts with its corporate customers, *id.* ¶¶ 32–41; (2) intentional interference with prospective economic advantage, *id.* ¶¶ 42–48; (3) unlawful, unfair, and fraudulent conduct in violation of the UCL, *id.* ¶¶ 49–63; and (4) declaratory judgment that BrandTotal has not breached any contract with Facebook because its access “has never been unlawful, misleading, or fraudulent,” because its products “have never impaired the proper working appearance or the intended operation of any Facebook product” or “accessed any Facebook product using automated means,” and because the individual users own the information at issue and have the right to decide

whether to share it with BrandTotal, *id.* ¶¶ 64–73. BrandTotal seeks both injunctive and compensatory relief. *Id.* at 23, ¶¶ A–E (Prayer for Relief).

B. Procedural History

Facebook initially filed state law claims against BrandTotal in the California Superior Court for San Mateo County, case number 20-CIV-04526, on October 1, 2020. Telscher Decl. (dkt. 27-4) ¶ 2; Kim Decl. (dkt. 44) ¶ 2. BrandTotal informed Facebook on October 8, 2020 of its intent to move for a TRO on October 13th or 14th. Telscher Decl. ¶ 4; Kim Del. ¶ 3 & Ex. 1. Facebook’s counsel asked BrandTotal to delay its TRO application, and BrandTotal asked, in exchange for such delay, for Facebook to agree to discuss the issues in the case and see if a resolution could be reached. Telscher Decl. ¶ 5; Kim Decl. ¶ 4 & Ex. 2. On the morning of that settlement conference, BrandTotal provided formal notice of its intent to move for a TRO. Telscher Decl. ¶ 6; Kim Dec. ¶ 5 & Ex. 3. According to BrandTotal’s attorney Rudolph Telscher, Facebook’s representatives at the settlement conference lacked authority to settle the case or provide assurances that would moot the need for a TRO. Telscher Decl. ¶ 7.

The same day, Facebook voluntarily dismissed its state court action and filed a complaint in this Court, adding new claims including its sole federal claim under the CFAA, before BrandTotal could move for a TRO in state court the following day. Telscher Decl. ¶ 8; Kim Decl. ¶ 8. According to Facebook’s attorney Jason Kim, the decision to add a CFAA claim was based on Facebook’s discovery that that BrandTotal’s browser extension had been relisted in the Chrome Web Store after Google had taken down an earlier version. Kim Decl. ¶ 8.

BrandTotal filed its present application two days later, on October 16, 2020. *See* Mot. (dkt. 27).

C. The Parties’ Arguments

1. BrandTotal’s Motion

BrandTotal seeks a TRO requiring Facebook to rescind its request that Google remove the UpVoice browser extension,⁶ reverse any technological measures that Facebook has used to block

⁶ Although other browser extensions were also removed, BrandTotal seeks a TRO only with respect to UpVoice

UpVoice from accessing its website, and restore BrandTotal’s and its principals’ pages on Facebook. *See* Proposed Order (dkt. 27-5). BrandTotal contends that this case is analogous to a recent Ninth Circuit decision affirming injunctive relief in favor of a company that collected data from publicly available LinkedIn profiles, *hiQ Labs, Inc. v. LinkedIn Corporation*, 938 F.3d 985 (2019). Mot. at 2. According to BrandTotal, any argument Facebook might make that it is protecting users’ privacy is belied by a history of privacy violations on Facebook’s part, including a five-billion-dollar Federal Trade Commission fine and a large class action settlement, thus supporting an inference that Facebook’s true motivation in this case is harming a potential competitor. *Id.*; *see also id.* at 6–7 (discussing congressional findings of monopolization and anticompetitive conduct by Facebook). BrandTotal contends that denying a TRO would “lead[] to the destruction of the business,” *id.* at 3, and that it meets the Ninth Circuit’s test for such relief based on a likelihood of immediate irreparable harm, the public interest favoring an injunction, the balance of equities tipping in BrandTotal’s favor, and a likelihood of success on (or at least serious questions going to) the merits of the case, *id.* at 8–9.

a. Success on the Merits

BrandTotal argues that it is likely to successfully defend against Facebook’s breach of contract claim because its product does not use the *type* of “automated” means that the terms of service are intended to prohibit—programs that scrape as much data as possible from an entire website. *Id.* at 9–10. According to BrandTotal, its browser extension operates only with a user’s consent and relies on the user’s deliberate conduct of browsing the Facebook Network, distinguishing it from malicious and more-fully-automated “scraper” programs like those used by Cambridge Analytica for purposes related to the 2016 election. *Id.* at 10.

Even if the Court construes Facebook’s prohibition of “automated means” (without Facebook’s permission) as encompassing BrandTotal’s product, BrandTotal argues that the prohibition is unenforceable because it purports to control users’ choices to share information they own. *Id.* at 10–11. BrandTotal cites intellectual property doctrines stemming from *Lear, Inc. v. Adkins*, 395 U.S. 653, 674–75 (1969), as well as California law providing that contracts may not contravene either express provisions of law or the *policies underlying* such provisions, Cal. Civ.

Code § 1667(2), as supporting its view that contractual provisions preventing users from sharing their own data are unenforceable because impair competition and the free flow of information. Mot. at 11–12. BrandTotal also cites the California Consumer Privacy Act (“CCPA”) as recognizing consumers’ ownership of their personal information, allowing businesses to offer consumers compensation for using that information, and prohibiting contracts that waive users’ rights under the statute. *Id.* at 12–13. BrandTotal contends that “[m]uch of what [it] collects are basic facts in the public domain,” and that courts have recognized that such facts cannot be restricted by copyright or a right of publicity. *Id.* at 13–14. BrandTotal also cites the Ninth Circuit’s concerns in *hiQ* regarding companies that host “vast amounts of public data” selectively excluding potential competitors, and thus potentially suppressing innovation. *Id.* at 14. Along the same lines, BrandTotal argues that Facebook’s exclusion of a competitor that seeks to compensate users for their information, while Facebook aggregates the same information for its own products and services that it sells to advertisers, violates the public policies underlying state and federal antitrust law. *Id.* at 14–17 (citing Telscher Decl. Ex. H, Facebook’s data policy, which permits such conduct by Facebook).

BrandTotal contends that it will likely prevail on Facebook’s claims under the CFAA and section 502(c) of the Penal Code, and for unjust enrichment, because it acted with users’ authorization—who in turn were authorized to access Facebook’s servers—and thus “has done nothing improper.” *Id.* at 17–18. BrandTotal argues that it will prevail on Facebook’s claim for interference with contract because it has not collected users’ login credentials, and thus did not induce users to breach the terms of service’s prohibition on sharing that information. *Id.* at 20.

With respect to its own counterclaims, BrandTotal argues that it is likely to prevail on its claims for intentional interference with contract and with prospective economic advantage because, by blocking access, Facebook interfered with BrandTotal’s contracts to provide analytics services to its customers. *Id.* at 18–19. BrandTotal contends that it will prevail on the “unlawful” prong of its UCL claim based on that intentional interference, and that Facebook’s conduct is also “unfair” because it is anticompetitive and “fraudulent” because it conflicts with representations in Facebook’s terms of service that users own their own data. *Id.* at 19–23.

b. Irreparable Injury, Balance of Equities, and Public Interest

BrandTotal asserts that it faces irreparable injury because it might be forced to close its business without access to data from Facebook’s products. *Id.* at 23–24. According to BrandTotal, Facebook would not face any significant harm if it were required to allow BrandTotal to continue operating during litigation in the same manner that it has already operated for years, which favors not only granting a TRO, but doing so without requiring any bond. *Id.* at 24–25. BrandTotal also contends that the public interest favors granting relief “[f]or the same reasons that make Facebook’s terms of service unenforceable.” *Id.* at 25.

2. Facebook’s Opposition

Facebook contends that BrandTotal has not met the requirement of irreparable injury because any risk of the demise of its business is speculative, and because the relief that it seeks would not actually redress its harm, which requires independent action by Google to reinstate the UpVoice browser extension. Opp’n at 9–12. Facebook also argues that the proposed TRO is insufficiently precise and would not be enforceable, *id.* at 10, and that BrandTotal’s delay of around two weeks in filing its present motion undermines its argument that immediate relief is critical, *id.* at 12–13.

Facebook contends that BrandTotal is unlikely to succeed on its intentional interference counterclaim because there is no evidence Facebook knew of any particular contracts affected by its denial of access, BrandTotal has not shown actual breach of a contract, Facebook acted with a legitimate business purpose of protecting user privacy and securing its platform, and any harm was caused by Google’s independent decision to remove UpVoice from its store. *Id.* at 13–15. Facebook argues that BrandTotal will not succeed on its UCL counterclaim because Facebook did not act unlawfully, has not violated the antitrust laws, and did not deceive users where its terms of use specifically provided that unauthorized automated access was prohibited. *Id.* at 15–17. Facebook also argues that it will likely succeed on its own claims against BrandTotal based on BrandTotal’s use of automated means to access password-protected data from Facebook’s products without Facebook’s permission, and based on BrandTotal inducing users to breach Facebook’s terms of service. *Id.* at 17–23.

Facebook contends that to “force Facebook to allow a non-compliant developer back on its platform” would be inequitable both with respect to the balance of equities between the parties, and with respect to the public interest. *Id.* at 23–24.

3. BrandTotal’s Reply

BrandTotal argues again in its reply that it faces imminent collapse as a business without a TRO allowing it access to data from Facebook’s platforms, among other intangible harm, and contends that the injury would likely be redressed by Facebook withdrawing any objection to Google allowing UpVoice in the Chrome Web Store. Reply (dkt. 50) at 3–7. BrandTotal also argues that it acted promptly in light of the complexity of the case and the parties’ discussions. *Id.* at 7–8.

BrandTotal contends that it is likely to prevail on both Facebook’s claims and its own counterclaims because its services do not constitute “automated means” as that term is used in Facebook’s terms of use, it obtained users’ permission to access their data, and allowing Facebook to restrict access to the data at issue under those circumstances would be anticompetitive and harmful to consumers’ rights to their own information. *Id.* at 9–14. In light of those concerns, and the degree of “power that companies like Facebook wield,” BrandTotal contends that the balance of equities and the public interest favor granting its request for a TRO. *Id.* at 14–15.

III. ANALYSIS

A. Legal Standard

The legal standard for a TRO is substantially identical to the standard for a preliminary injunction. *See Stuhlbarg Int’l Sales Co., Inc. v. John D. Brush & Co., Inc.*, 240 F.3d 832, 839 n.7 (9th Cir. 2001).⁷ “A preliminary injunction is an extraordinary remedy never awarded as of right.” *Winter v. Nat. Res. Defense Council, Inc.*, 555 U.S. 7, 24 (2008). “A plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his

⁷ A TRO issued “without written or oral notice to the adverse party or its attorney” is subject to additional limitations. *See* Fed. R. Civ. P. 65(b). As Facebook received notice of BrandTotal’s motion and has participated in briefing and argument, those limitations do not apply here.

favor, and that an injunction is in the public interest.” *Id.* at 20. Irreparable harm must be likely—it is no longer sufficient to grant a preliminary injunction upon a mere showing of a “possibility” of irreparable harm when the other factors weigh heavily in favor of the plaintiff. *Alliance for the Wild Rockies v. Cottrell*, 632 F.3d 1127, 1132 (9th Cir. 2011). Nonetheless, the Ninth Circuit still evaluates the likelihood of success on a “sliding scale.” *Id.* A TRO or preliminary injunction may be warranted upon a showing of “serious questions going to the merits” as well as “a hardship balance that tips sharply toward the plaintiff,” so long as the plaintiff is likely to suffer irreparable harm and the injunction or restraining order is in the public interest. *Id.*

B. *HiQ v. LinkedIn*

BrandTotal contends that this case is analogous to the Ninth Circuit’s decision affirming injunctive relief in *hiQ Labs, Inc. v. LinkedIn Corporation*, 938 F.3d 985 (2019). The plaintiff in that case, hiQ, used automated computer programs to “scrape[] information that LinkedIn users have included on public LinkedIn profiles, including name, job title, work history, and skills,” and “then use[d] that information, along with a proprietary predictive algorithm, to yield ‘people analytics,’ which it [sold] to business clients.” *Id.* at 991. The access at issue concerned only profiles that LinkedIn users elected to “ma[ke] visible to the general public.” *Id.* at 990. LinkedIn, which competed with hiQ to sell products derived from information its users included in their profiles, sent hiQ a cease-and-desist letter asserting violations of the CFAA and other laws, and claiming to have implemented technical measures to block hiQ’s access to LinkedIn’s website. *Id.* at 991–92.

HiQ brought suit for declaratory judgment that LinkedIn could not invoke the CFAA or other authority on which it relied, and for injunctive relief on a number of claims under California law, and sought a TRO. *See id.* at 992. The parties agreed to convert hiQ’s request for a TRO into a motion for a preliminary injunction. *Id.* The district court—the Honorable Edward Chen, of this district—“granted hiQ a preliminary injunction, concluding that the balance of hardships tips sharply in hiQ’s favor and that hiQ raised serious questions on the merits.” *Id.* at 992–93. The Ninth Circuit affirmed, focusing on hiQ’s claim for intentional interference with contract and LinkedIn’s defense based on the CFAA. *See id.* at 993–1005.

The Ninth Circuit first affirmed the determination that hiQ showed a threat of irreparable injury based threats to “the survival of its business”—including contracts it would not be able to honor, loss of interest in an ongoing financing round, and the departure of employees—because hiQ’s business model was based entirely on access to LinkedIn profile data. *Id.* at 993–94. The court noted that although a threat of monetary injury generally is not sufficient to support a preliminary injunction, longstanding Ninth Circuit precedent has recognized that “showing a threat of ‘extinction’ is enough to establish irreparable harm, even when damages may be available and the amount of direct financial harm is ascertainable.” *Id.* at 993 (citing *Am. Passage Media Corp. v. Cass Commc’ns, Inc.*, 750 F.2d 1470, 1474 (9th Cir. 1985)).

Next, the Ninth Circuit “conclude[d] that the district court’s determination that the balance of hardships tips sharply in hiQ’s favor [was] not ‘illogical, implausible, or without support in the record,’” because neither LinkedIn nor its users had a strong privacy interest in profile data that was made available to the public. *Id.* at 994–95. The court noted concerns that even users who made their profiles available for public viewing might not wish for others (such as their employers) to have easy methods of knowing when the users *changed* information in their profiles, but held that such interests were not particularly strong where nothing prevented employers from monitoring employees’ profiles for changes, and LinkedIn itself offered products that could be used for that sort of monitoring. *Id.*

Turning hiQ’s likelihood of success on the merits, the panel held that hiQ made a sufficient showing of each element of a claim for intentional interference with contract under California law: (1) “a valid contract between plaintiff and a third party,” by showing several contracts with customers that paid for hiQ’s data analytics services; (2) “defendant’s knowledge of this contract,” by showing that hiQ publicly advertised its business model and responded to LinkedIn’s cease-and-desist letter by identifying specific customers; (3) “defendant’s intentional acts designed to induce a breach or disruption of the contractual relationship,” based on LinkedIn’s threats to invoke federal law and technological measures to block hiQ’s access; (4) “actual breach or disruption of the contractual relationship,” by preventing hiQ from accessing the LinkedIn data on which hiQ relied for its product; and (5) “resulting damage,” in the form of lost revenue when hiQ

could not sell its products. *Id.* at 996–97 (citation and internal quotation marks omitted).

In response to LinkedIn’s assertion of legitimate business purpose as a defense to that claim, the court applied a broad balancing test, based in precedent from California courts, weighing the legitimate interests furthered by the defendant’s conduct against “the importance of the interest interfered with,” looking to factors including harm to competition, good faith, and whether the conduct is a “recognized trade practice.” *Id.* at 997–98. The court determined that hiQ had a strong interest in honoring its existing contracts, LinkedIn had a “relatively weak” interest in preventing hiQ’s use of public profile data, LinkedIn’s selective blocking of access was not a recognized trade practice, and there was some evidence to suggest that LinkedIn blocked hiQ’s access in order to introduce a new data analytics product that competed with hiQ. *Id.* The Ninth Circuit therefore agreed with the district court that hiQ had shown serious questions going to the merits of its tortious interference claim.

Based on a thorough review of precedent interpreting the CFAA, the Ninth Circuit held that “it appears that the CFAA’s prohibition on accessing a computer ‘without authorization’ is violated when a person circumvents a computer’s generally applicable rules regarding access permissions, such as username and password requirements, to gain access to a computer,” and conversely, that it “is likely that when a computer network generally permits public access to its data, a user’s accessing that publicly available data will not constitute access without authorization under the CFAA.” *Id.* at 1003. The court concluded that hiQ “raised serious questions about whether LinkedIn may invoke the CFAA” with respect to data from public profiles, and thus found no basis to reverse the preliminary injunction on account of that statute. *Id.* at 1004.

Finally, the Ninth Circuit concluded that although “there are significant public interests on both sides, the district court properly determined that, on balance, the public interest favors hiQ’s position,” because “giving companies like LinkedIn free rein to decide, on any basis, who can collect and use data—data that the companies do not own, that they otherwise make publicly available to viewers, and that the companies themselves collect and use—risks the possible creation of information monopolies that would disserve the public interest.” *Id.* at 1005.

LinkedIn’s petition for certiorari challenging the preliminary injunction remains pending

before the Supreme Court. *See LinkedIn Corp. v. hiQ Labs, Inc.*, No. 19-1116 (U.S.). The district court recently granted a motion by LinkedIn to dismiss hiQ’s antitrust claims (but granted leave to amend on “theories of unilateral refusal to deal and the essential facilities doctrine”) and denied the motion as to hiQ’s interference claims, holding that those claims were not barred by the *Noerr-Pennington* doctrine. *See hiQ Labs, Inc. v. LinkedIn Corp.*, No. 17-cv-03301-EMC, 2020 WL 5408210 (N.D. Cal. Sept. 9, 2020).

C. Irreparable Harm

Monetary injury alone cannot generally establish the irreparable harm necessary to support preliminary injunctive relief, but a “threat of ‘extinction’”—i.e., a party being driven out of business—can meet that standard. *HiQ*, 938 F.3d at 993 (quoting *Am. Passage*, 750 F.2d at 1474; and citing *L.A. Mem’l Coliseum Comm’n v. Nat’l Football League*, 634 F.2d 1197, 1202 (9th Cir. 1980)). “[I]ntangible injuries, such as damage to ongoing recruitment efforts and goodwill, qualify as irreparable harm.” *Rent-A-Ctr., Inc. v. Canyon Television & Appliance Rental, Inc.*, 944 F.2d 597, 603 (9th Cir. 1991). The Ninth Circuit has held that a district court does not abuse its discretion in finding irreparable harm where damages from such injuries “would be difficult to value.” *Id.*

Facebook contends that BrandTotal’s purported evidence of a threat to its ongoing business is conclusory, speculative, and insufficiently precise as to how long BrandTotal could continue to operate without access to data from Facebook’s products. Opp’n at 11. Last year, Chief Judge Hamilton denied a TRO under similar circumstances, holding that a CEO’s declaration that the plaintiffs would “soon reach a tipping point where [they] can no longer operate” was “inherently speculative” because the plaintiffs failed to “offer any indication about their financial strength or the likelihood that they will dissolve as going concerns at any particular point in time.” *Stackla, Inc. v. Facebook Inc.*, No. 19-cv-05849-PJH, 2019 WL 4738288, at *5 (N.D. Cal. Sept. 27, 2019).⁸ Judge Hamilton also noted that the plaintiffs failed to identify

⁸ Facebook cites a press release as evidence that BrandTotal recently raised \$12 million in venture capital funding, providing a URL for a PR Newswire website but no evidence in the record. Opp’n at 11. While courts may in some circumstances take judicial notice of the *existence* of public media reports, courts cannot accept as true the facts stated in such reports. *See Von Saher*

specific customers they had lost or were likely to lose in the absence of relief. *Id.* She concluded that in the absence of clear evidence of *imminent* failure of their business, the plaintiffs had not met their burden to obtain a “temporary restraining order, the purpose of which is to address only harms caused by actions likely to occur between the time of its filing and a preliminary injunction hearing.” *Id.* at *3, *5.

BrandTotal’s evidence here is stronger than in *Stackla*, in that BrandTotal presents communications from specific existing customers expressing concern about Facebook’s allegations, and from specific potential customers suspending or postponing their negotiations with BrandTotal, as well as some information about lost venture capital investment. Leibovich Decl. (dkt. 27-3) ¶¶ 33–35, 39–43, 52–55 & Exs. B–D.

Other aspects of the record here are more similar to *Stackla*. BrandTotal’s CEO Alon Leibovich states that although “BrandTotal has some investment funds in reserve, without the ability to conduct business, BrandTotal will be forced to immediately lay off employees,” and its “inability to raise any new capital will irreparably impact [its] growth trajectory and viability.” *Id.* ¶ 56. Leibovich concludes that BrandTotal “cannot long survive” without data collected from Facebook using UpVoice. *Id.* ¶¶ 61–62.

Like in *Stackla*, Leibovich has not addressed any timeline under which BrandTotal would be forced to cease operations. Even assuming for the sake of argument that Leibovich’s declaration might show likely irreparable harm in the absence of relief before *trial*—itself not entirely clear, absent evidence of how long BrandTotal could survive—the Court cannot say whether expedited relief in the form of a TRO, as opposed to a preliminary injunction considered in the normal course, is necessary to prevent such harm. *See Stackla*, 2019 WL 4738288, at *3–5; *see also AboveGEM, Inc. v. Organo Gold Mgmt., Ltd.*, No. 19-cv-04789-PJH, 2019 WL 3859012, at *5 (N.D. Cal. Aug. 16, 2019) (denying a TRO where the plaintiff did “not offer any indication

v. Norton Simon Museum of Art at Pasadena, 592 F.3d 954, 960 (9th Cir. 2009). A press release might warrant different analysis if it is a statement of a party opponent, but in the absence of any evidence in the record regarding this purported press release, the Court cannot determine whether the information on the third-party website is authentic and BrandTotal actually made the statement at issue. The Court therefore declines to consider it.

of *when* it would be driven out of business, or underlying financial information that would demonstrate imminent, irreparable harm” (emphasis added)); *Int’l Medcom, Inc. v. S.E. Int’l, Inc.*, No. 15-cv-03839-HSG, 2015 WL 7753267, at *5 (N.D. Cal. Dec. 2, 2015) (denying a preliminary injunction where the plaintiff failed to show that its “survival [was] a matter of weeks or months”). Even after Facebook raised this issue in its opposition brief, Leibovich’s reply declaration states only that BrandTotal “cannot long survive without a TRO,” and that its board of directors might determine that continued operations are not worthwhile. Leibovich Reply Decl. (dkt. 50-2) ¶ 9. Beyond that speculative statement, there is no evidence that any member of the board has actually resolved to shut down BrandTotal in the absence of relief, much less on any particular schedule. To the extent that Leibovich’s reply declaration addresses BrandTotal’s financial circumstances, he suggests that it currently has sufficient funding to continue operations for perhaps up to a year—or potentially less in light of reductions in revenue and the resources required to litigate this case, but BrandTotal is not at risk of immediately depleting its reserves. *Id.* ¶ 8.

Leibovich states that *layoffs* would be immediate without relief. Although the Court is aware of no authority specifically holding that layoffs alone constitute irreparable injury sufficient to support a TRO or preliminary injunction, they are comparable to intangible injuries such as harm to recruitment that courts have held sufficient. *See, e.g., Regents of Univ. of Cal. v. Am. Broad. Cos., Inc.*, 747 F.2d 511, 520 (9th Cir. 1984). Without better evidence of BrandTotal’s financial condition, however, it is not clear whether such layoffs would be based on BrandTotal’s business judgment that its available funds are better spend elsewhere while operations are disrupted—and thus merely a choice that BrandTotal might make in response to monetary harm—or if BrandTotal would lack the resources to continue to pay those employees and remain a going concern. In the absence of authority so holding, the Court declines to endorse a rule that any monetary loss that might induce a party to lay off employees constitutes irreparable harm, which would threaten to swallow the rule that monetary damages are not sufficient to support preliminary injunctive relief. *See Am. Passage*, 750 F.2d at 1473 (holding that a plaintiff failed to show irreparable injury despite losing “a substantial amount of business,” sustaining “large losses,” and forecasting such losses to continue).

While BrandTotal has not shown that it falls within the rule addressing threats of extinction, it has shown massive disruption of its business. According to Leibovich, BrandTotal has lost access to “95% of the data necessary . . . to provide [its] services to [its] customers.” Leibovich Decl. ¶ 37. Leibovich also states that a particular “well renowned market research firm, whom [BrandTotal has] a longstanding business partnership with, has frozen all work.” *Id.* ¶ 42. Leibovich’s declaration further identifies a number of large potential customers that were in negotiations with BrandTotal but have suspended talks. *Id.* ¶¶ 39–40. Evidence submitted with BrandTotal’s reply shows that one customer declined to renew its contract on short notice, shortly after Facebook brought its state court action and Google removed UpVoice from its store. Leibovich Reply Decl. Ex. P.

The Ninth Circuit has recognized, separately from cases dealing with the potential demise of a business, that “[e]vidence of threatened loss of prospective customers or goodwill certainly supports a finding of the possibility of irreparable harm.” *Stuhlbarg Int’l Sales Co. v. John D. Brush & Co.*, 240 F.3d 832, 841 (9th Cir. 2001). Some district court decisions have nevertheless found such harms insufficient where a value could be placed on the lost relationships. *See Int’l Medcom*, 2015 WL 7753267, at *5 (citing *Telephia Inc. v. Cuppy*, No. C 04-03508 SI, 2005 WL 588441, at *4 (N.D. Cal. Mar. 11, 2005)). Under the circumstances of this case, where BrandTotal is a small and growing business that has been forced to suspend a major portion of its operations, the Court concludes that the potential harms from “loss of prospective customers or goodwill,” *Stuhlbarg Int’l*, 240 F.3d at 841, are sufficiently “difficult to value,” *Rent-A-Ctr.*, 944 F.2d at 603, to establish irreparable harm.

Some courts have held that, as a corollary to the rule that a party seeking an injunction must show irreparable harm in the absence of relief—and related to the issue of Article III standing—the moving party must also show that granting relief would prevent such harm. *See Sierra Club v. U.S. Dep’t of Energy*, 825 F. Supp. 2d 142, 153 (D.D.C. 2011). Facebook argues that even if BrandTotal has shown irreparable harm, it has not shown that the relief it seeks would remedy that harm, because allowing the UpVoice extension on the Chrome Web Store is exclusively within non-party Google’s control. Opp’n at 9–10. The parties agree that Google

only removed UpVoice from its Chrome Web Store after Facebook filed its state court action against BrandTotal. *See* Karve Decl. (dkt. 42) ¶ 14. Facebook alleged in that complaint that it had asked Google multiple times in the preceding month to remove BrandTotal’s browser extensions. *See* Mehta Decl. (dkt. 40) Ex. 2 (state court complaint) ¶ 56. After initially removing the extension from its store, Google approved the listing of another version of UpVoice on October 14, 2020—which BrandTotal’s vice president Oren Dor states was not meant to go live, but only submitted for approval so that BrandTotal could quickly return to service if its TRO were granted, and which BrandTotal changed to “unlisted” when it realized the error more than a day later. Dor Decl. (dkt. 27-2) ¶¶ 24–28.⁹ Given that Google has already approved that new instance of UpVoice for listing on the Chrome Web Store at least once, it is reasonable to infer that Google would allow it to remain if Facebook withdrew any objection or request for its removal. *See Utah v. Evans*, 536 U.S. 452, 464 (2002) (holding that a plaintiff has standing where an injunction “would amount to a significant increase in the likelihood that the plaintiff would obtain relief that directly redresses the injury suffered”).

Facebook also argues that BrandTotal’s delay of around two weeks in seeking a TRO after Facebook filed its state court complaint and Google removed the UpVoice extension belies any need for emergency belief. Opp’n at 12–13. In light of the complexity of the issues implicated, as well as the parties’ efforts to discuss potential resolutions, the Court does not fault BrandTotal for that delay.

BrandTotal’s arguments for irreparable harm are limited to the effects of losing access to data collected from Facebook’s products, which resulted from Google taking down the UpVoice browser extension. *See* Mot. at 23–24. BrandTotal has not specifically addressed any irreparable harm resulting from Facebook’s removal of BrandTotal’s and its principals’ pages on Facebook. *See id.*; *see also id.* at 25 (asking to “reinstate the status quo so that BrandTotal has access to UpVoice user-authorized content”). In the absence of any argument that irreparable harm resulted

⁹ Dor’s declaration does not account for another period when, according to Facebook researcher Sanchit Karve, a version of UpVoice was available on the Chrome Web Store from October 12, 2020 to October 14, 2020, but that discrepancy does not undermine the inference that Google would allow the extension but for Facebook’s objection. *See* Karve Decl. ¶ 14.

from that removal, BrandTotal’s request for an order requiring Facebook to restore those pages is DENIED. *See id.* at 25; Proposed Order ¶ 1(c).¹⁰ The remainder of this order addresses only Facebook’s efforts to block the use of UpVoice, including requesting that Google remove it from the Chrome Web Store, and BrandTotal’s request that it be restored.

D. Likelihood of Success

Each party argues that it is likely to succeed on each of the claims and counterclaims in the case. The Court focuses on BrandTotal’s counterclaims, as those would be the basis for BrandTotal obtaining affirmative relief in this case, although Facebook’s claims are relevant to the extent that they could serve as affirmative defenses to BrandTotal’s claims.

1. BrandTotal’s Counterclaim for Interference with Contract

BrandTotal asserts counterclaims for intentional interference with contract, and intentional interference with prospective economic advantage. “The elements which a plaintiff must plead to state the cause of action for intentional interference with contractual relations are (1) a valid contract between plaintiff and a third party; (2) defendant’s knowledge of this contract; (3) defendant’s intentional acts designed to induce a breach or disruption of the contractual relationship; (4) actual breach or disruption of the contractual relationship; and (5) resulting damage.” *HiQ*, 938 F.3d at 995–96 (quoting *Pac. Gas & Elec. Co. v. Bear Stearns & Co.*, 50 Cal. 3d 1118, 1126 (1990)). While the typical case involves actual breach, the element of “disruption” of a contract can also be satisfied “where the plaintiff’s performance has been prevented or rendered more expensive or burdensome.” *Id.* at 996 n.8 (citation and internal quotation marks omitted).

BrandTotal argues that, like in *hiQ*, it has established a likelihood of success on those elements based on Facebook blocking BrandTotal’s access to the data it would need to fulfill its contracts with existing customers of its advertising analytics product. *See* Mot. at 18–19. Facebook argues that BrandTotal cannot show knowledge, or actual breach or disruption. Opp’n

¹⁰ Thus far, BrandTotal also has not specifically addressed or attempted to justify its vice president Dor’s purported creation of accounts using false names, in apparent violation of Facebook’s terms of service. *See* Karve Decl. ¶ 34; Answer (dkt. 23) ¶ 61 (admitting that a BrandTotal employee created the accounts at issue).

at 13–14. With respect to disruption, Leibovich’s states that BrandTotal can no longer access the data on which it relies for the analysis it contracted to sell to its customers. Leibovich Decl. ¶ 37 (stating that due to lack of access, BrandTotal “cannot provide the promised content”). BrandTotal is therefore likely able to show that its “performance has been prevented or rendered more expensive or burdensome.” See *hiQ*, 938 F.3d at 996 n.8.

On the element of knowledge, BrandTotal cites no evidence that Facebook knew of a *particular* contract with a *particular* customer. But under California law, “the defendant need not know exactly who is a party to the contract, so long as he knows he is interfering with a contractual relationship.” *Altera Corp. v. Clear Logic, Inc.*, 424 F.3d 1079, 1092 (9th Cir. 2005). As BrandTotal notes, Facebook included the following allegation in its complaint evincing knowledge that BrandTotal sold services based on the data it collected:

[BrandTotal] used the data collected by the malicious extensions to sell “marketing intelligence,” and other services through the website brandtotal.com. BrandTotal publicly stated that it used the data obtained through the malicious extensions to provide marketing insights about users and advertisers. Exs. 5 and 11.

Compl. ¶ 47; see also Mehta Decl. Ex. 2 (state court complaint) ¶ 45. Exhibit 5 to Facebook’s complaint is a screenshot of BrandTotal’s website, which includes the statement that “[m]any of the most recognizable consumer brands use our competitive marketing intelligence platform to discover marketing threats and opportunities in real time.” Compl. Ex. 5; see also Mehta Decl. Ex. 2 (state court complaint, which includes the same exhibit). BrandTotal is therefore likely to succeed in showing that Facebook knew BrandTotal had entered contracts where its performance depended on the data it collected.

The more significant issue with respect to this claim is Facebook’s argument that it acted with a “legitimate business purpose,” which can serve as a defense to interference. See Mot. at 14. “Under California law, a legitimate business purpose can indeed justify interference with contract, but not just any such purpose suffices.” *HiQ*, 938 F.3d at 997. Courts must determine whether the defendant’s interest outweighs societal interests in stability of contracts (the defendant’s mere pursuit of economic advantage generally does not), “whether the means of interference involve no more than recognized trade practices,” “whether the conduct is within the realm of fair

competition,” and—most importantly—“whether the business interest is pretextual or asserted in good faith.” *Id.* (citations and internal quotation marks omitted).

BrandTotal raises serious questions as to this defense for largely the same reasons addressed in *hiQ*. Facebook’s data policy suggests that it sells marketing intelligence services potentially in competition with BrandTotal’s product. *See* Telscher Decl. Ex. H (data policy); Mot. at 16 (quoting provisions of the policy indicating that, among other things, Facebook “provide[s] advertisers with reports about the kinds of people seeing their ads” and “share[s] information about [users] with companies that aggregate it to provide analytics and measurement reports to [Facebook’s] partners”). To the extent that Facebook’s efforts to restrict BrandTotal’s access might be motivated to stifle competition, it would raise some of the same concerns as in *hiQ*, where the Ninth Circuit determined that for companies “whose servers hold vast amounts of public data” to “selectively . . . ban only potential competitors from accessing and using that otherwise public data” . . . “may well be considered unfair competition under California law.” *HiQ*, 938 F.3d at 998. This case differs in that some of the information at issue is not “public,” but BrandTotal is likely correct that the advertisements themselves are essentially public, *see* Compl. ¶¶ 17–19 (Facebook’s allegations discussing its public library of all ads on its services), that the users who consent to use BrandTotal’s browser extension have the most significant interest in the data in their own profiles,¹¹ and that Facebook has not articulated a significant privacy or intellectual property interest in any data outside of those categories, such as the “advertising interests” that Facebook generates for (and shares with) its users, and the metrics of engagement (likes, comments, etc.) on particular advertisements. So long as BrandTotal’s browser extension works as intended and represented, it threatens interests at most only

¹¹ Despite the CCPA’s general purpose of granting consumers greater control over how their personal information is used, BrandTotal has not cited any provision of that statute that specifically requires Facebook to provide the sort of access at issue here. *See* Mot. at 12–13 (addressing provisions of the statute defining “personal information,” providing that companies may compensate users for their personal information, and providing that any contract purporting to waive a right under the statute is unenforceable). The fact that the statute allows companies to provide financial compensation to consumers for collection of their personal information, Cal. Civ. Code § 1798.125(b)(1), does not by its terms require *other* companies that have collected users’ information to make it available to the company offering compensation.

marginally greater than those the Ninth Circuit found “relatively weak” in *hiQ*. See 938 F.3d at 998.

On the other hand, Facebook’s general interest in policing access to the password-protected portions of its networks is far greater than LinkedIn’s interest in restricting access to otherwise public pages in *hiQ*. See *Stackla*, 2019 WL 4738288, at *6 (concluding that “Facebook’s ability to decisively police the integrity of its platforms is without question a pressing public interest”); cf. *hiQ*, 938 F.3d at 992 (rejecting an argument that the plaintiff could collect suitable data from sources other than LinkedIn, because “Facebook data, by contrast, is not generally accessible”). Users on Facebook’s networks choose share information with specific people, and could reasonably be expected to rely on Facebook’s privacy settings and terms of use to prevent automated collection of that information by third parties. See, e.g., Clark Decl. (dkt. 41) ¶¶ 5(b)–(d).

Facebook is bound by an order from an FTC enforcement action requiring it to enforce its terms of use against third parties that have access to users’ information. Clark Decl. Ex. 1.

Among other things, the FTC order requires Facebook to take the following measures:

Specifically with respect to any Covered Third Party that obtains or otherwise has access to Covered Information from Respondent for use in an independent, third-party consumer application or website, such safeguards shall include:

a. Requiring an annual self-certification by each Covered Third Party that certifies: (i) its compliance with each of Respondent’s Platform Terms; and (ii) the purpose(s) or use(s) for each type of Covered Information to which it requests or continues to have access, and that each specified purpose or use complies with Respondent’s Platform Terms;

b. Denying or terminating access to any type of Covered Information that the Covered Third Party fails to certify pursuant to Part VII.E.1.a.(ii) above, or, if the Covered Third Party fails to complete the annual self-certification, denying or terminating access to all Covered Information unless the Covered Third Party cures such failure within a reasonable time, not to exceed thirty (30) days;

c. Monitoring Covered Third Party compliance with Respondent’s Platform Terms through measures including, but not limited to, ongoing manual reviews and automated scans, and regular assessments, audits, or other technical and operational testing at least once every twelve (12) months; and

d. Enforcing against any Covered Third Party violations of Respondent's Platform Terms based solely on the severity, nature, and impact of the violation; the Covered Third Party's malicious conduct or history of violations; and applicable law;

Id. at 9. For the purpose of that order, "Covered Third Party" is defined as:

any individual or entity that uses or receives Covered Information obtained by or on behalf of Respondent outside of a User-initiated transfer of Covered Information as part of a data portability protocol or standard, other than:

(1) a service provider of Respondent that (i) uses the Covered Information for and at the direction of Respondent and no other individual or entity and for no other purpose; and (ii) does not disclose the Covered Information, or any individually identifiable information derived from such Covered Information, except for, and at the direction of, Respondent, for the purpose of providing services requested by a User and for no other purpose; or

(2) any entity that uses the Covered Information only as reasonably necessary: (i) to comply with applicable law, regulation, or legal process, or (ii) to enforce Respondent's terms of use, or (iii) to detect, prevent, or mitigate fraud or security vulnerabilities.

Id. at 3, ¶ E (line breaks added).

As BrandTotal tentatively agreed at the hearing, *see* Hearing Tr. (dkt. 57) at 8:19–9:1, it appears to meet that definition, and there is no evidence that it has certified compliance as required under the FTC's order. Facebook therefore had a legitimate business interest—i.e., complying with its legal obligations—in preventing BrandTotal's access. Facebook also believes that it was required to report BrandTotal's access to the FTC as a "scraping incident," and its Director of Product Management states in a declaration that Facebook will submit such a report. Clark Decl. ¶ 12. Clark is unaware of any request from BrandTotal to access Facebook's data with Facebook's permission. *Id.* ¶ 14.

Facebook's interest in securing its platform to comply with legal obligations and protect users' privacy is further supported by evidence that BrandTotal's products have posed risks to privacy. According to a third party report addressing a number of BrandTotal products other than UpVoice, which Facebook researcher Sanchit Karve reviewed while investigating BrandTotal's products, the technique that BrandTotal used to anonymize user's profile ID numbers (which could be used to link the collected data to a particular user) was "very weak" and "could be reversed very quickly" with widely available tools. Karve Decl. ¶ 25. Karve states that Facebook

1 personnel determined that another BrandTotal product, “Anonymous Story Viewer for Instagram,”
2 collected a wide range of data and transmitted it to a third-party server in plain text, without
3 anonymization. *Id.* ¶ 22. That product also collected and transmitted the user’s “session token”
4 and “session ID,” which a third party could use to access Instagram as if they were the user. *Id.*
5 ¶ 23. Although those issues do not specifically pertain to the UpVoice product, Facebook’s
6 perception that BrandTotal had a history of collecting user data in ways that posed risks to security
7 and privacy supports a legitimate business interest in policing BrandTotal’s access to Facebook’s
8 platforms.

9 As for UpVoice specifically, while users of that extension generally consented to sharing
10 their own demographic information with BrandTotal, the extension could collect information from
11 other users who did not know of or consent to that collection if it was installed on a shared
12 computer. *See Clark Decl.* ¶ 5(c). Despite Facebook raising that concern in its opposition brief,
13 Opp’n at 6, BrandTotal does not address the issue in its reply.¹² Facebook’s Director of Product
14 Management also states in his declaration that Facebook has a practice of “enforce[ing] its anti-
15 scraping policies regardless of who is doing it or how they are using the scraped information,”
16 because “it can be difficult to determine whether scraping is engaged in for benign or malicious
17 purposes.” *Id.* ¶ 9.

18 The Court concludes that Facebook likely has at least some degree of legitimate business
19 interest in safeguarding user privacy and security by preventing unapproved programs from
20 automatically collecting data after users have logged into Facebook’s social networks, in order to
21 comply with its obligations under the FTC order, avoid other potential liability for data breaches,
22 and maintain public confidence in its products. *See Clark Decl.* ¶¶ 5(a), 11–12. That interest
23 supports requiring companies like BrandTotal who seek to collect such data to coordinate with
24 Facebook and obtain approval, even when those companies have no malicious intent and have
25 endeavored to protect users’ privacy and obtain their consent. Facebook provides application

26
27 ¹² At the hearing, BrandTotal’s attorney did not dispute that UpVoice could capture information
28 from non-consenting users of shared computers, but asserted that BrandTotal is “not aware of this
shared-computer thing being much of an issue.” *See Hearing Tr.* at 4:17–5:24; *see also id.* at
23:14–26:13.

programming interfaces (“APIs”) and other “approved means” for users to share their data with third parties. Clark Decl. ¶ 4. The record indicates that, thus far, BrandTotal has not requested access through those means. *Id.* ¶ 14.

“Whether an intentional interference by a third party is justifiable depends upon a balancing of the importance, social and private, of the objective advanced by the interference against the importance of the interest interfered with, considering all circumstances including the nature of the actor’s conduct and the relationship between the parties.” *HiQ*, 938 F.3d at 997 (quoting *Herron v. State Farm Mut. Ins. Co.*, 56 Cal. 2d 202, 206 (1961)). To the extent that Facebook’s denial of access to BrandTotal was based on BrandTotal’s failure to coordinate with Facebook and seek approval through established channels, and on Facebook’s perception that BrandTotal had a history of collecting user data in irresponsible ways, the balance tips in favor of allowing Facebook to enforce its prohibition against unapproved automated access. On the other hand, to the extent that Facebook might have been motivated by a desire to prevent BrandTotal from competing against Facebook in the market for advertising analytics, the balance would favor granting relief in order to foster competition and innovation, and allow BrandTotal to honor its contracts with its customers. *See hiQ*, 938 F.3d at 997–98. The apparent failure of *either* party to initiate dialog as to how BrandTotal might obtain approval from Facebook to conduct that business leaves an open question of Facebook’s intent, and whether Facebook would approve access by BrandTotal if it worked within Facebook’s protocols for authorizing access. The Court concludes that BrandTotal has raised serious questions as to the merits of this claim, but on the current record, it has not established a likelihood of success.¹³

¹³ Facebook also argues that any potential interference with BrandTotal’s contracts had a legitimate business purpose because “Facebook was entirely justified in incidentally interfering with a contract that threatened ‘a prior contract of [its] own.’” Opp’n at 14 (quoting *Richardson v. La Rancherita*, 98 Cal. App. 3d 73, 81 (1979)) (alteration in original). As discussed below in the context of BrandTotal’s claim for declaratory judgment, the UpVoice extension very likely breached Facebook’s terms of use. Facebook’s interest in enforcing its own terms reinforces the conclusion that BrandTotal has not shown a likelihood of success. *Richardson* recognized, however, that even where a defendant seeks to enforce its own contract, the “determinative question” is the defendant’s good faith. 98 Cal. App. 3d at 81. BrandTotal has also raised real issues of the extent to which Facebook can enforce its terms of use in a manner that stifles competition. *See* Mot. at 11–17. Facebook’s terms of use do not negate the serious issues BrandTotal has shown on its claim for intentional interference with contract.

2. BrandTotal’s Counterclaim for Interference with Advantage

The parties do not draw any significant distinctions between BrandTotal’s claims for intentional interference with contract and intentional interference with prospective economic advantage, except that the latter claim requires showing “‘an independently wrongful act.’” Mot. at 18 (quoting *Reeves v. Hanlon*, 33 Cal. 4th 1140, 1145 (2004)); see Opp’n at 13–15 (addressing these claims together); Reply at 13 (same). The Court concludes that, for the reasons discussed above in the context of interference with contract, BrandTotal has shown at most serious issues going to the merits of its claim for interference with advantage.

3. BrandTotal’s Counterclaim for Unfair Competition

California’s UCL broadly prohibits unlawful, unfair, and fraudulent business acts. *Kor. Supply Co. v. Lockheed Martin Corp.*, 29 Cal.4th 1134, 1143 (2003). “Unlawful acts are anything that can properly be called a business practice and that at the same time is forbidden by law . . . be it civil, criminal, federal, state, or municipal, statutory, regulatory, or court-made, where court-made law is, for example a violation of a prior court order.” *Sybersound Records, Inc. v. UAV Corp.*, 517 F.3d 1137, 1151 (9th Cir. 2008) (ellipsis in original) (citations and internal quotation marks omitted). “Unfair acts among competitors means ‘conduct that threatens an incipient violation of an antitrust law, or violates the spirit or policy of those laws because its effects are comparable to or the same as a violation of the law, or otherwise significantly threatens or harms competition.’” *Id.* at 1152 (quoting *Cel-Tech Commc’ns, Inc. v. L.A. Cellular Tel. Co.*, 20 Cal. 4th 163, 187 (1999)). “Finally, fraudulent acts are ones where members of the public are likely to be deceived.” *Id.*

With respect to the “unlawful” prong, BrandTotal rests this claim on its intentional interference with contract claim discussed above. BrandTotal has shown serious issues going to the merits of that claim, but not a likelihood of success. With respect to the “unfair” prong, BrandTotal has again shown no more than serious issues, because although Facebook’s enforcement efforts could be seen as intended to block a potential competitor from the market for advertising analytics, Facebook has significant countervailing interests in enforcing its terms of service to prevent unauthorized automated collection of the data available to logged-in users of its

services.

BrandTotal argues that Facebook blocking its access is “fraudulent” because, according to BrandTotal, Facebook’s terms of service recognize that users retain ownership of their own data. Mot. at 22–23; Reply at 14. Assuming for the sake of argument that BrandTotal’s characterization of the terms of service is accurate, restricting the *means* that users may engage in to extract that data from Facebook’s servers does not clearly conflict with recognizing ownership of the data. Facebook’s clear prohibition of automated means without permission also tends to negate any potential reliance on broad statements of user ownership as suggesting the contrary, that automated means could be used *without* permission. BrandTotal has shown at most serious issues going to this claim, not a likelihood of success.

4. BrandTotal’s Counterclaim for Declaratory Judgment

BrandTotal seeks declaratory judgment that it has not breached Facebook’s terms of service because its process of obtaining data is not “automated,” its access has never been “unlawful, misleading, or fraudulent,” and it has not “impaired the proper working appearance or the intended operation of any Facebook product.” Counterclaim ¶¶ 64–73. Although BrandTotal has argued in the context of other claims that Facebook’s terms of service are unenforceable, this counterclaim does not seek such a declaration. *See id.*

BrandTotal’s position that its access is not “automated” defies any reasonable meaning of that term. BrandTotal suggests that an earlier version of the terms of service suggests a narrower meaning of the term by including the parenthetical “(such as harvesting bots, robots, spiders, or scrapers)” after the term “automated means.” Mot. at 10 (quoting Telscher Decl. Ex. I). Regardless of whether BrandTotal’s product would fall outside of those examples—which is not clear on the current record—BrandTotal is not accused of breaching the 2017 terms; it is accused of breaching the current terms, which do not include the parenthetical at issue and instead refer only to “automated means.” *See* Compl. ¶ 26; Duffey Decl. (dkt. 43) Ex. 1 § 3.2.3 (“You may not access or collect data from our Products using automated means (without our prior permission)

...”).¹⁴ After users install the UpVoice browser extension, it automatically collects data while the users browse the Facebook Network and certain other websites, including not only information that users see on their screens, but also information that the browser extension itself automatically requests from the website. *See* Dor Decl. ¶¶ 14–20; Karve Decl. ¶ 17 (addressing the particular categories of information that UpVoice automatically collected as a user browsed the Facebook Network). BrandTotal also collects data regarding the “number of likes, shares, and comments” on advertisements “*separate* from [its] panelist [i.e., user] collection,” belying the implication in BrandTotal’s briefs that all data collection derives from user activity. Dor Decl. ¶ 21 (emphasis added); *cf.*, *e.g.*, Mot. at 10 (“If these deliberate steps [by users] are not taken, no information is collected.”). The fact that BrandTotal does not attempt to “survey[] Facebook’s entire site” does not make its access any less automated. *Cf.* Mot. at 10.

BrandTotal asserts that any practical method of collecting data from Facebook’s products requires “some degree of automation,” thus conceding “some degree of automation” in its own products that perform that service. *See id.* at 11. There might be edge cases where it would be difficult to determine if a particular method of accessing an inherently technological product like the Facebook Network was “automated”—for example, a user recording video of their screen while browsing the website. This is not such a case. BrandTotal designed a computer program to systematically identify, capture, and transmit certain types of data from Facebook’s products without user intervention. Because BrandTotal used “automated means” to access and collect data from Facebook’s website without obtaining Facebook’s permission as required by the terms of service, the Court concludes that BrandTotal has not shown a likelihood of success, or even serious issues, on its claim for declaratory judgment that it did not breach those terms. Because the record tends to suggest that BrandTotal breached at least the provision regarding automated access, the Court does not reach the parties’ arguments as to other contract terms at issue.

To the extent BrandTotal’s declaratory judgment counterclaim could be construed as

¹⁴ Some of the exhibits to Michael Duffey’s declaration compress what should be many pages of text to a single column on a single letter-sized page. Those exhibits would be unusable in hard copy form, and the resolution of Exhibit 2 is too low to be legible even in its digital form. Facebook’s counsel is admonished to provide any future exhibits in a functional format.

seeking a declaration that Facebook’s terms of service are unenforceable as against public policy, BrandTotal has not shown a likelihood of success because, as discussed above in the context of Facebook’s “legitimate business purpose” defense to BrandTotal’s intentional interference claim, a significant public policy supports allowing Facebook to police automated access to its password-protected platforms. BrandTotal has therefore shown at most significant issues going to whether Facebook’s terms are enforceable, which does not add to the analysis of the present motion beyond the significant issues BrandTotal has shown for intentional interference.

E. Balance of Equities

The balance of equities requires a court to consider “the interests of all parties and weigh the damage to each.” *CTIA - The Wireless Ass’n v. City of Berkeley*, 928 F.3d 832, 852 (9th Cir. 2019) (citation and internal quotation marks omitted).

Facebook has legitimate interests in maintaining public confidence in its products and avoiding potential liability for data privacy breaches. Ordering Facebook to allow access by BrandTotal, without BrandTotal completing Facebook’s usual vetting process and using the standard APIs for obtaining users’ permission to access their personal data, risks some degree of harm to public confidence in Facebook’s data protection. As for potential liability for a breach, the current record does not indicate major vulnerabilities that would result from the UpVoice product specifically—except perhaps as to the users who have installed UpVoice, and others who might share their computers—and Facebook is unlikely to face liability for complying with an order of this Court requiring it to grant access. The Court also notes that Facebook has endured unauthorized access by BrandTotal for some time, including the several-month period since it began its investigation of BrandTotal in April of this year, without suffering any significant harm that it has identified in the current record.¹⁵ Nevertheless, the potential harm to Facebook’s reputation that could result from granting BrandTotal’s motion—and ordering Facebook to tolerate automated data collection from password-protected portions of its network, by a third

¹⁵ As perhaps a countervailing consideration to any harm it might suffer, Facebook could stand to benefit if BrandTotal’s products incentive users to frequently interact with Facebook’s networks, or if they enhance the value of advertising that third parties pay Facebook to host on those networks.

party Facebook has not vetted and approved—is serious.

On the other hand, BrandTotal is not able to operate its business while it lacks access to Facebook’s products. As discussed above in the context of irreparable injury, BrandTotal is losing customers, faces new difficulty attracting investment, and is at risk of eventually shutting down. Weighing the potential harm to only the parties to this case,¹⁶ BrandTotal faces far greater consequences from the denial of a TRO than Facebook would suffer if the TRO were granted and BrandTotal’s access restored pending the conclusion of litigation. The balance of equities therefore tips in favor of BrandTotal. The Court assumes for the sake of argument that it tips “sharply.”

F. Public Interest

“The public interest inquiry primarily addresses impact on non-parties rather than parties,” and “embodies the Supreme Court’s direction that ‘in exercising their sound discretion, courts of equity should pay particular regard for the public consequences in employing the extraordinary remedy of injunction.’” *Bernhardt v. Los Angeles Cty.*, 339 F.3d 920, 931–32 (9th Cir. 2003) (quoting *Weinberger v. Romero-Barcelo*, 456 U.S. 305, 312 (1982)). The public interest in this case requires a balancing of the interests addressed by the Ninth Circuit in *hiQ*, favoring open access to information and competition for data analytics services, and those identified by Judge Hamilton in *Stackla*, favoring proactive data and privacy protection by companies like Facebook. On balance, the Court is not persuaded that the public interest favors the relief that BrandTotal seeks, requiring Facebook to provide immediate access to an automated data collection program that Facebook has not vetted.

Addressing similar issues in *Stackla*, Judge Hamilton held as follows:

Awarding injunctive relief at this stage would compel Facebook to permit a suspected abuser of its platform and its users’ privacy to continue to access its platform and users’ data for weeks longer, until a preliminary injunction motion could be resolved. Moreover, as precedent within Facebook’s policy-setting organization and potentially with other courts, issuing an injunction at this stage could

¹⁶ Public interest—including, here, the interests of individual Facebook and BrandTotal users, who are not parties to the case—is also highly significant to the Court’s analysis, but better addressed below in the separate element of the TRO test that looks to that issue.

handicap Facebook’s ability to decisively police its social-media platforms in the first instance. Facebook’s enforcement activities would be compromised if judicial review were expected to precede rather than follow its enforcement actions.

Although the public certainly has some interest in avoiding the dissolution of companies and the accompanying loss of employment, Facebook’s ability to decisively police the integrity of its platforms is without question a pressing public interest. In particular, the public has a strong interest in the integrity of Facebook’s platforms, Facebook’s policing of those platforms for abuses, and Facebook’s protection of its users’ privacy. Congress’s ample attention to such abuse is more than enough to demonstrate the importance of those interests to the public, as are Facebook’s recent interactions with the FTC. . . .

Stackla, 2019 WL 4738288, at *6.¹⁷ As Judge Hamilton noted, Facebook’s FTC violation stemmed from allegations of “[1] maintaining deceptive settings that misled users about how to protect their information from being shared by Facebook with third-party developers of apps . . . [2] promising to stop giving app developers access to the data of app users’ Friends starting in 2014, when in fact many app developers continued to have such access past that date . . . [and 3] inconsistently enforcing its privacy policies against app developers who violated those policies.” *Id.* (quoting *United States v. Facebook, Inc.*, No. 19-cv-02184-TJK, ECF Doc. No. 4 (D.D.C. July 25, 2019)) (alterations in original).

BrandTotal’s access to Facebook users’ data circumvents Facebook’s privacy settings. Although users separately consent to sharing most if not all of the data at issue when they install the UpVoice browser extension, BrandTotal’s method of operating outside of Facebook’s platform and APIs means that users who later review their Facebook privacy settings will not see BrandTotal among the third parties with whom they have agreed to share information, and any subsequent changes that users make to their Facebook privacy settings will not limit the information that is shared with BrandTotal. Such circumstances could render Facebook’s privacy settings “deceptive” and create risk of users being “misled”—some of the concerns that spurred

¹⁷ Another decision from this district, on a motion for default judgment, recently granted Facebook a permanent injunction forbidding access by defendants accused of scraping user data from Facebook using browser extensions, citing *Stackla*’s analysis of Facebook’s interest in securing its platform. *Facebook, Inc. v. Sluchevsky*, No. 19-cv-01277-JSC, 2020 WL 5823277, at *9 (N.D. Cal. Aug. 28, 2020), *report and recommendation adopted*, No. 19-cv-01277-YGR, 2020 WL 5816578 (N.D. Cal. Sept. 30, 2020).

the FTC’s enforcement action.¹⁸ Moreover, requiring Facebook to set aside in this instance its normal requirement that third parties seek and obtain Facebook’s permission before collecting data using automated means would *mandate* the sort of inconsistent enforcement of Facebook’s policies that also concerned the FTC.

When it comes to advertising data—as opposed to user data—there are significant countervailing concerns. As the Ninth Circuit noted in *hiQ*, “giving [social networking] companies . . . free rein to decide, on any basis, who can collect and use data—data that the companies do not own, that they otherwise make publicly available to viewers, and that the companies themselves collect and use—risks the possible creation of information monopolies that would disserve the public interest.” *HiQ*, 938 F.3d at 1005. Facebook does not own the contents of advertisements placed on its networks, and already makes all such ads available for public viewing. *See* Compl. ¶ 17. While Facebook notes that its advertisers maintain intellectual property rights to the content of their ads, it has not suggested that BrandTotal’s use of that content is anything but fair use. Facebook also has not suggested that it “owns” the related information that BrandTotal collects about advertisements, such as the number of likes and comments, or which users are presented with a given ad. Allowing a third party like BrandTotal to compete with Facebook to provide data analytics services about advertising campaigns on Facebook’s networks—advertising for which Facebook is already compensated by the advertisers—would be consistent with a strong public interest in “maximizing the free flow of information on the Internet” and fostering competition and innovation. *See hiQ*, 938 F.3d at 1004. On balance, however, the Court is not satisfied that those interests wholly prevent Facebook from vetting or regulating third parties that seek to automatically collect large quantities of user data from nonpublic portions of Facebook’s networks.

¹⁸ UpVoice’s apparent ability to collect data from other users of shared computers who have not themselves consented to sharing data with BrandTotal raises even greater concerns about deception. BrandTotal argued at the hearing that such collection is “innocuous” because it includes only “deidentified demographic information,” Hearing Tr. at 24:22–25:8, but the fact remains that Facebook users have at least some interest in preventing the surreptitious collection of personal information that, using Facebook’s privacy settings, they may have chosen to share only with select other users of the Facebook Network. BrandTotal’s decoupling of that demographic information from a user’s name does not entirely negate the user’s privacy interest.

Expedited judicial proceedings are not an efficient mechanism to adjudicate in the first instance potential data privacy risks from products that automatically collect Facebook users' data. The record suggests that BrandTotal has operated, at least for the most part, in good faith, and likely poses no greater risk than described above, but courts generally lack the technical expertise to evaluate such risks on a blank slate. And if Facebook could not take steps to block access by third party developers unless it first builds a strong case of actual harm to its users—without the benefit of the developer working with Facebook to explain its product's operation and safeguards—malicious actors would likely enjoy longer periods of access to users' data before facing any enforcement. Requiring a company seeking such access to coordinate with Facebook and address potential concerns before obtaining access ensures that, if such a company believes Facebook's denial of access is impermissible, a court evaluating such a claim will benefit from a fuller evidentiary record, presented by parties who understand each other's products and positions.

Under the circumstances of this case, where BrandTotal built its business on ignoring Facebook's prohibition on automated access without permission, created separate architecture to collect users' Facebook profile data in ways not reflected in those users' Facebook privacy settings, and now requests an immediate order preventing Facebook from taking any steps to limit its access despite an FTC order requiring Facebook to enforce its terms of use and police such access, the Court concludes that the public interest requires denying the extraordinary relief BrandTotal seeks.

IV. CONCLUSION

BrandTotal has shown a risk of irreparable harm in the absence of relief, serious issues going to the merits of its claims, and a balance of hardships that tips in its favor, perhaps sharply so. The public interest, however, weighs against granting the relief that BrandTotal seeks.¹⁹

///

¹⁹ Because the Court denies BrandTotal's motion based on public interest, the Court does not reach Facebook's argument that the order BrandTotal seeks—compelling Facebook to "take other reasonable actions in communication with Google" to ensure reinstatement of the UpVoice browser extension—would not meet the standards of specificity and enforceability required for an injunction under Rule 65(d) of the Federal Rules of Civil Procedure. See Opp'n at 10.

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

BrandTotal’s motion for a TRO is therefore DENIED.

IT IS SO ORDERED.

Dated: November 2, 2020



JOSEPH C. SPERO
Chief Magistrate Judge