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 TO DISMISS COUNTERCLAIMS

Re: Dkt. No. 77

I. INTRODUCTION

Plaintiff Facebook, Inc. brought this action asserting various 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 the Court previously denied BrandTotal's application for a temporary restraining order ("TRO"). Facebook now moves to dismiss BrandTotal's counterclaims for failure to state a claim under Rule 12(b)(6) of the Federal Rules of Civil Procedure. The Court held a hearing on February 19, 2021. For the reasons discussed below, Facebook's motion is GRANTED, and BrandTotal's counterclaims are DISMISSED, with leave to amend some counterclaims as discussed below. The shall file a joint letter proposing a schedule on February 22, 2021.[2]

[1] Unimania, Inc. is a software development subsidiary of BrandTotal Ltd.

[2] The parties have consented to the jurisdiction of the undersigned magistrate judge for all

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 issue of fact that might be disputed at a later stage of the case.

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 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:

[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

> 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 payment for UpVoice users, by allowing Ads Feed users to review lists of ads they had seen in the last ninety days so that users could return to ads that interested them, and by telling users that they would serve as "panelists" to influence corporate marketing decisions. *Id.* ¶¶ 43, 44, 49, 56.

BrandTotal analyzed and sold the data that it obtained from users to corporate clients. *Id.* ¶ 37. BrandTotal used different trade names for its browser extensions (which gathered data) and its marketing intelligence product (which incorporated that data), and advertised its products to both potential individual users (who might install the browser extensions and provide data) and potential corporate clients (who might purchase data) on the Facebook Network. *Id.* ¶¶ 39–40, 42, 47.

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

On September 30, 2020, Facebook disabled BrandTotal's accounts on Instagram and the Facebook Network and instated other technological measures to block BrandTotal's access to Facebook's products. *Id.* ¶ 58. On October 1, 2020, Facebook filed a civil action against BrandTotal in California state court alleging that the browser extensions breached Facebook's terms of service. *Id.* ¶ 59.[4] Later that day, Google removed the browser extensions from its Chrome Web Store, which disabled their functionality. *Id.* ¶ 60. On October 3, 2020, BrandTotal's chief product officer created accounts on Instagram and the Facebook Network using false names. *Id.* ¶ 61. On October 12, 2020, BrandTotal introduced a new UpVoice browser extension on the Chrome Web Store, listing the developer of the extension as "UpVoice Team." *Id.* ¶ 62. According to Facebook, the new UpVoice extension—like its predecessors—collected data when users accessed the Facebook Network and returned that data to BrandTotal, including 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;

[4] Facebook voluntarily dismissed its state court action before bringing the present action in this

(3) unauthorized access in violation of the Computer Fraud and Abuse Act ("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 Counterclaims

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 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

[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

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.