

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA

META PLATFORMS, INC.,  
Plaintiffs,  
v.  
BRIGHT DATA LTD.,  
Defendants.

Case No. 23-cv-00077-EMC

**ORDER DENYING META’S MOTION  
FOR PARTIAL SUMMARY  
JUDGMENT; AND GRANTING  
BRIGHT DATA’S MOTION FOR  
SUMMARY JUDGMENT**

Docket Nos. 75, 105

This is a data-scraping case brought by Meta Platforms, Inc. (“Meta”) against Bright Data Ltd. (“Bright Data”). Before the Court is Bright Data’s motion for summary judgment and Meta’s cross-motion for partial summary judgment. Meta seeks partial summary judgment in its favor on its breach of contract claims as to the issue of liability. Bright Data seeks summary judgment in its favor as to Meta’s breach of contract claims. For the reasons below, the Court **DENIES** Meta’s cross-motion for partial summary judgment and **GRANTS** Bright Data’s motion for summary judgment.

**I. FACTUAL AND PROCEDURAL BACKGROUND**

A. The Parties

1. Meta

Plaintiff Meta is a company headquartered in California that operates, among other products, Facebook and Instagram. Docket No. 1 (“Compl.”) at ¶¶ 4, 14, 15. Facebook is a social networking website and mobile application that allows its users to “create their own personal profiles and connect with each other.” *Id.* at ¶ 14. When a user creates a Facebook account, they are required to create a password and register with their name, email, or mobile phone number,

1 date of birth, and gender. *Id.* at ¶ 17. Meta also operates Instagram, a photo and video sharing  
 2 website and mobile application. *Id.* at ¶ 15. Instagram users can create a personal profile, post  
 3 photos and videos to their profile, and “view, comment on, and like posts shared by others on  
 4 Instagram.” *Id.* To create an Instagram account, users must register with their email address and  
 5 create a username and password, which then allows them to create user profiles and add  
 6 information about themselves to those profiles. *Id.*

7 Meta allows users to control how to customize their profiles and how much information  
 8 they would like to include in their profiles. *Id.* at ¶ 18. For example, someone who is not logged  
 9 into Facebook or Instagram can only view a “limited amount of content.” *Id.* at ¶ 16. They can  
 10 only see content that users have allowed the public to see, but not content that is set to “private” or  
 11 limited to specific audiences such as a user’s friends. *Id.* at ¶ 30b. After a non-logged in  
 12 individual views a certain amount of information or tries to engage with the content such as  
 13 “lik[ing]” or commenting on a photo, Meta’s “lockout mechanism” redirects them to a login  
 14 screen that prompts them to either create an account or log into an existing account. *Id.* at ¶¶ 16,  
 15 30b.

16 Meta has approved certain means for Facebook and Instagram users to share data with  
 17 third parties, including through Application Programming Interfaces (“APIs”). *Id.* at ¶ 19.  
 18 “Authorized” APIs can access data from Facebook and Instagram, but they must agree to Meta’s  
 19 Terms of Service (the “Facebook Terms”) and Instagram’s Terms of Use (the “Instagram Terms”)  
 20 (together, the “Terms”) to do so. *Id.*

21 However, Meta has also developed a variety of technologies to combat *unauthorized*  
 22 *automated* data scraping. *Id.* at ¶ 30. Data scraping is a means to extract data from a website or  
 23 app, usually using automation. *Id.* at ¶ 29. The technological restrictions Meta uses to combat  
 24 scraping and “suspicious” activity include its lockout mechanism; imposing rate and data limits  
 25 that restrict the number of times anyone can interact with Meta’s computers and view certain types  
 26 of data; subjecting individuals to technical checks called “reCAPTCHAs” or “CAPTCHAs” to  
 27 confirm they are human; and deploying machine-learning models and tools that detect and block  
 28 automated scraping and suspicious account activity including “inauthentic behavior, compromised

accounts, and automated accounts. *Id.* at ¶ 30.

## 2. Bright Data

Defendant Bright Data is a company with its principal place of business in Israel that operates the website brightdata.com. *Id.* at ¶ 5. Bright Data is an “internet company” that “searches the web for information” and sells data collected from various websites, including Facebook, Instagram, Twitter, Amazon, Airbnb, LinkedIn, Etsy, and Bing, among others, and scraping tools and services. Docket No. 75 (Bright Data’s Mot. for Summ. J.) (“Bright Data’s Mot.”)) at 3; Compl. at ¶ 6. Bright Data’s customers include “Fortune 500 companies, academic institutions, and small businesses, who use Bright Data’s technologies to search for, retrieve, and synthesize Internet data.” *Id.* at ¶ 4.

Bright Data offers a variety of services to customers. First, its “proxy network service” is an “intermediary server, device, or server application that sits between an end user and a website or other server.” Kol Decl. Ex. 1 at ¶¶ 3-4. The proxy network allows Bright Data customers to “browse the [I]nternet anonymously by redirecting their communications through other third-party devices that are under contract with Bright Data.” *Id.* at ¶ 6. In addition, Bright Data’s proxy customers may use a Bright Data tool called “Web Unlocker,” a tool Bright Data claims is designed to prevent website operators like Meta from “us[ing] various techniques to blacklist members of the public” from accessing public information on the Internet. *Id.* at ¶¶ 14-15 (emphasis in original). Second, Bright Data’s “self-managed data collector” service includes a tool named the Web Scraper Integrated Development Environment (“Webscraper IDE”). *Id.* at ¶ 20. The Webscraper IDE helps programmers “develop their search codes, including certain templates, debugging tools, and pre-coded, commonly used functions.” *Id.* at ¶¶ 22-23. When customers use the proxy network service and the self-managed data collector service, customers decide which specific web pages they would like to search (including “automated and non-automated searching” in the case of the proxy network). *Id.* at ¶¶ 10, 12-13, 24-25. Bright Data claims these services are used only for “‘logged-off’ or non-member access to public websites.” *Id.* at ¶ 13. In short, Bright Data asserts it only scrapes publicly available data. It does not scrape data which is only accessible to a logged-in Meta user. It does not scrape, *e.g.*, password protected

1 data.

2 Bright Data also provides a “managed data collector” service. Customers who use this  
3 service do not conduct the searches themselves. Kol Decl. at ¶¶ 31-34. Instead, they make  
4 specific requests to Bright Data, and Bright Data prepares “customized data sets ... based on its  
5 own searches” to respond to the request. *Id.* at ¶ 27. To “streamline” its own search design  
6 process, Bright Data has developed “Web scraper” templates to create custom searches for  
7 customers, including the “Facebook Scraper” and the “Instagram Scraper.” *Id.* at ¶ 28; *see also*  
8 Compl. at ¶¶ 36-37. Lastly, Bright Data “designs, creates, and sells,” its “standardized” or pre-  
9 made datasets. *Id.* at ¶ 34. A standardized dataset customer simply purchases an “off-the-shelf”  
10 dataset rather than one that responds to a specific customer request. *Id.*

11 Bright Data claims that its services allow customers to search for “public data that others  
12 choose to make available on the Internet.” *Id.* at ¶ 2. It also claims that none of its services  
13 require customers to be Meta users or have a user account, “even when searching Meta websites.”  
14 *Id.* at ¶ 4. In addition, Bright Data claims that its services “do not require customers to provide  
15 Meta log-in information; they do not ask customers to provide Meta log-in information; they do  
16 not contain any fields in which customers can input Meta log-in information; and they do not auto-  
17 populate any fields on Meta sites with Meta log-in information.” *Id.*

18 B. Meta’s Allegations

19 Meta alleges that Bright Data “developed and used unauthorized automation software to  
20 scrape data from Facebook and Instagram, including users’ profile information, followers, and  
21 posts that users have shared with others”; that Bright Data advertised the sale of such scraped data;  
22 and that Bright Data “developed, tested, and sold tools and services that enable others to scrape  
23 [such data] and to avoid detection by Meta and other websites.” *Id.* at ¶ 2. Meta alleges that  
24 Defendant’s conduct “violated several Facebook and Instagram terms and policies” even when  
25 Bright Data scrapes only publicly available data. Meta alleges Bright Data refused to permanently  
26 cease these activities when demanded by Meta to do so. *Id.* at ¶ 3. Meta brought its lawsuit for  
27 damages and injunctive relief to halt Bright Data’s alleged violations of Facebook and Instagram’s  
28 terms and policies, claiming both breach of contract and tortious interference with contract. *Id.* at

¶¶ 2, 69-70.

Bright Data moved for summary judgment on Meta’s breach of contract claim, asserting that its scraping publicly available data is not prohibited by the Meta, Facebook, or Instagram Terms. It raises the defenses of lack of mutual assent and lack of consideration and disputes the application of Meta’s Terms to any scraping done after terminating its Facebook and Instagram accounts. *See* Bright Data’s Mot. Meta filed a cross-motion for partial summary judgment as to liability for breach of contract and an opposition to Bright Data’s motion for summary judgment, arguing that Meta’s Terms created a valid and enforceable contract, and that Bright Data was bound by and breached the Terms by its scraping activities. *See* Docket No. 105 (Meta’s Opp. To Bright Data’s Mot. for Summ. J. & Cross-Mot. for Partial Summ. J. (“Meta’s Opp.”)). These motions are now pending before the Court.

C. Undisputed Facts

1. Contract Existence and Enforceability

Bright Data admits that it maintained “one or more” Facebook and Instagram user accounts between April 1, 2021, and December 4, 2022, and it also concedes that it was “subject to the applicable Israeli [Terms] in effect” at that time.” Docket No. 105-1 (Declaration of Ari Holtzblatt in Support of Plaintiff’s Cross-Motion for Summ. J. and Opp. To Defendant’s Mot. for Summ. J (“Holtzblatt Decl.”)) Ex. D at 8. Bright Data claims that its Facebook and Instagram accounts were “corporate accounts” for advertising its services but did not use these accounts for scraping data. Holtzblatt Decl. Ex. D at 9; Kol Decl. at ¶¶ 48-53.

On November 29, 2022, Meta’s Privacy and Data Policy Manager conducted a video conference with Bright Data executives and sent an email quoting Meta’s Terms. Docket No. 75-1 (Declaration of David A. Munkittrick in Support of Bright Data’s Mot. for Summ. J. (“Munkittrick Decl.”)) Ex. 3. The email demanded that Bright Data, within 48 hours, “[r]emove and cease the selling of any user data” obtained from Facebook and Instagram, “[r]emove and disable any access to existing datasets of Meta users’ data,” and “[s]top scraping and facilitating the scraping of Meta users’ data.” *Id.* It stated that failure to cooperate with the deadline specified could result in enforcement action. *Id.*

On December 1, 2022, Bright Data responded to Meta’s letter by proposing a “two-week standstill” during which it would not “sell any data sets derived from Meta public-generated data to any third-party and [would] remove them from [its] data set marketplace.” *Id.* Meta responded, also on December 1, 2023, agreeing with Bright Data’s proposal, but claiming that Bright Data’s continued access and collection of data from Meta products and services was “unauthorized and is a violation of Facebook’s and Instagram’s terms.” *Id.*

On December 4, 2022, Bright Data’s CEO, Or Lechner, sent an email to Meta’s Privacy and Data Policy Manager and other Bright Data staff. *Id.* Ex. 4. In the letter, Lechner noted that any accounts Bright Data created on Facebook and Instagram “were not used in connection with, and are completely unrelated to,” the activities mentioned in Meta’s prior letter. *Id.* Lechner further claimed that Bright Data had “exercised [its] right to terminate those accounts and [was] no longer a ‘user’ of Meta’s products and services and [was] not now subject to Meta’s user terms.” *Id.* In addition, Lechner said the letter served to provide Meta with notice that “Bright Data affirmatively rejects and has not consented to any agreement to your user terms in any context for any reason.” *Id.*

On January 6, 2022, Meta’s counsel, WilmerHale, sent Bright Data a letter “reiterat[ing]” that Bright Data must “immediately cease” selling Facebook and/or Instagram user data, disable any access to such data, delete any such data possessed by Bright Data, and refrain from scraping and facilitating the scraping such data, or Meta would take action to enforce its rights. *Id.* Ex. 5. Meta filed its lawsuit that same day, claiming both breach of contract and tortious interference.

In response, Bright Data’s counsel, the Proskauer firm, sent a letter to Meta’s counsel on January 13, 2023, reiterating that Bright Data had “terminate[d] [its] accounts” with Meta and providing a screenshot of one such example. *Id.* Ex. 6 (alterations in original). Bright Data also provided screenshots suggesting that Meta had disabled, as of January 7, 2023, at least one Bright Data Facebook account. *Id.* Ex. 6. Bright Data filed the present motion for summary judgment on Meta’s breach of contract claim on June 12, 2023.

Bright Data continued to scrape data after purportedly terminating its Facebook and Instagram accounts: “Today, Bright Data uses automated means to search for information that

1 ‘people without Facebook or Instagram accounts or who are not logged into their accounts are able  
2 to view.’” Bright Data’s Mot. at 3-4 (quoting Compl. at ¶ 30b).

3 2. Contract Breach

4 Bright Data admits that “it used automated means to search for and collect publicly  
5 available information that Meta voluntarily posted to Facebook, and which is available to  
6 members of the public without logging-in to or using a Meta user account.” Holtzblatt Decl. Ex.  
7 D at 8.

8 Bright Data admits it “designs, creates, and sells” datasets made up of aggregated data  
9 from Facebook and Instagram. Docket No. 51-1 (Declaration of David A. Munkittrick in Support  
10 of Bright Data’s Mot. to Dismiss) Ex. 1 (Declaration of Ron Kol (“Kol Decl.”)) at ¶ 34, although  
11 it claims it only sells “public” data. *Id.*

12 D. Purportedly Disputed Facts

13 Bright Data claims it only scraped (and scrapes) logged-off “public” data. Bright Data’s  
14 Mot. at 2. Meta “disputes as a factual matter that Bright Data is engaged in ‘public search.’”  
15 Declaration of Ari Holtzblatt (“Holtzblatt Decl.”) Docket No. 105-1, ¶ 21. Bright Data also denies  
16 that it used any Facebook or Instagram account for the scraping activities alleged in the  
17 Complaint. Holtzblatt Decl. Ex. D at 9. It says it only used these accounts to advertise its  
18 scraping services. Kol Decl. at ¶¶ 48-53. As discussed below, the Court finds on the record  
19 before the Court there is no genuine issue of fact whether Bright Data scraped non-public data  
20 while logged in—it did not.

21 **II. LEGAL STANDARD**

22 A “court shall grant summary judgment [to a moving party] if the movant shows that there  
23 is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of  
24 law.” Fed. R. Civ. P. 56(a). An issue of fact is genuine only if there is sufficient evidence for a  
25 reasonable jury to find for the nonmoving party. *See Anderson v. Liberty Lobby, Inc.*, 477 U.S.  
26 242, 248-49 (1986). “The mere existence of a scintilla of evidence . . . will be insufficient; there  
27 must be evidence on which the jury could reasonably find for the [nonmoving party].” *Id.* at 252.  
28 At the summary judgment stage, evidence must be viewed in the light most favorable to the

1 nonmoving party and all justifiable inferences are to be drawn in the nonmovant's favor. *See id.* at  
2 255.

3 Where a defendant moves for summary judgment based on a claim for which the plaintiff  
4 bears the burden of proof, the defendant need only point to the plaintiff's failure "to make a  
5 showing sufficient to establish the existence of an element essential to [the plaintiff's] case."  
6 *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986). Once the moving party has made this  
7 showing, the burden then shifts to the party opposing summary judgment to proffer "'specific facts  
8 showing there is a genuine issue for trial.'" *Id.* (citation omitted); *see also* Fed. R. Civ. P. 56(c)(1)  
9 (providing that a party alleging a fact is genuinely disputed "must support the assertion by . . .  
10 citing to particular parts of materials in the record").

11 When parties submit cross-motions for summary judgment, "[e]ach motion must be  
12 considered on its own merits." *Celotex*, 477 U.S. at 322; *see also* 10A Charles Alan Wright,  
13 Arthur R. Miller & Mary Kay Kane, Fed. Prac. & Proc. § 2720, at 335-36 (3d ed.1998) ("The  
14 court must rule on each party's motion on an individual and separate basis, determining, for each  
15 side, whether a judgment may be entered in accordance with the Rule 56 standard."). "In fulfilling  
16 its duty to review each cross-motion separately, the court must review the evidence submitted in  
17 support of each cross-motion." *Fair Hous. Council of Riverside Cnty., Inc. v. Riverside Two*, 249  
18 F.3d 1132, 1136 (9th Cir. 2001). Furthermore, as the Ninth Circuit has noted:

19  
20 It is well-settled in this circuit and others that the filing of cross-  
21 motions for summary judgment, both parties asserting that there are  
22 no uncontested issues of material fact, does not vitiate the court's  
responsibility to determine whether disputed issues of material fact  
are present. A summary judgment cannot be granted if a genuine  
issue as to any material fact exists.

23 *United States v. Fred A. Arnold, Inc.*, 573 F.2d 605, 606 (9th Cir. 1978); *see also Chevron USA,*  
24 *Inc. v. Cayetano*, 224 F.3d 1030, 1037 & n. 5 (9th Cir. 2000) (acknowledging the district court's  
25 responsibility to analyze whether the record on cross-motions for summary judgment demonstrates  
26 the existence of genuine issues of material fact, even in those cases in which both parties believe  
27 that there are no material factual issues).

### III. META’S MOTION FOR PARTIAL SUMMARY JUDGMENT

Meta seeks partial summary judgment in its favor on the issue of liability. It asks the Court to rule that: (1) Bright Data is, and continues to be, contractually bound by the Meta Terms because it used those services with actual knowledge of the Terms and Meta performed by offering those services and (2) Bright Data sold and continues to sell data obtained from Facebook and Instagram in violation of the Meta Terms. *See* Docket No. 105-4 (“Meta’s Prop’d Order”). Bright Data contests these claims on the grounds that (1) Meta’s Terms do not prohibit public search of websites without a user account and (2) Meta’s Terms do not prohibit Bright Data from offering its proxy and scraping services to its customers. *See* Docket No. 75-2 (“Bright Data’s Prop’d Order”).

#### A. Liability

Under California law, a “cause of action for damages for breach of contract is comprised of the following elements: (1) the contract, (2) plaintiff’s performance or excuse for nonperformance, (3) defendant’s breach, and (4) the resulting damages to plaintiff.” *Armstrong Petroleum Corp. v. Tri-Valley Oil & Gas Co.*, 116 Cal. App. 4th 1375, 1391 n.6 (2004).

Because Meta has not met its burden to show it is entitled to judgment based on undisputed facts, the Court **DENIES** Meta’s motion for partial summary judgment on the issue of liability for breach of contract.

#### 1. No Evidence of Logged-in Scraping

A key issue the parties dispute is whether Bright Data scraped data while logged into Facebook and Instagram accounts and thereby accessed data beyond that which is publicly viewable. Although Bright Data acknowledges that it scrapes (and has scraped) data, it claims that it only scrapes publicly available data, not data that is behind a log-in screen that is, *e.g.*, password protected. Bright Data’s Mot. at 2. Meta disputes Bright Data’s claim that it only accesses, collects, and sells public data. Meta’s Opp. at 16. In other words, Meta disputes Bright Data’s claim that it only scrapes data while logged off. However, Meta has not presented evidence sufficient to raise a reasonable inference that Bright Data scraped data while logged into an account and thereby accessed non-public data.

Despite having access to its own computer infrastructure as well as an extensive discovery opportunities, Meta has not shown any data that its users' protected data—data not publicly available—was scraped and sold by Bright Data.

Instead of any specific evidence of collection by Bright Data of non-public user information, Meta simply claims that Bright Data has collected and sold “vast” amounts of data from Facebook and Instagram. Opp. at 12. Meta states that “Bright Data offers for sale a dataset of Instagram user data containing 615 million records for \$860,000.” Mot. at 5; Docket No. 105-2 (Declaration of Tushar Karumudi (“Karumudi Decl.”)) Ex. A. The data set includes fields from Instagram users' profiles, including full name, ID, country code, region, post count, biography, business category, hashtags, followers, following, posts, profile image, highlights, verification status, business email, and business addresses. Mot. at 5; Karumudi Decl., Ex. A. But the screenshot of the dataset in question that accompanies the declaration clearly states that it is made up of “public web data” from “public profiles.” Karumudi Decl. Ex. A. While a declaration by a member of its “Anti-Scraping Team,” *id.* at ¶ 3, states that that anti-scraping analysts spent “hours” investigating Bright Data's interactions with Facebook and Instagram, including a sample of records from Bright Data's “Instagram accounts dataset,” *id.* at ¶ 6, the declaration does not establish that this was data that can *only* be accessed through a user account. Meta has not presented evidence to show that this data was unavailable to the public and has presented no evidence contradicting Bright Data's assertion that the data scraped was publicly available without logging in. Kol Decl. Ex. 1 at ¶¶ 29-30.<sup>1</sup>

---

<sup>1</sup> Bright Data's Chief Technology and Security Officer offers the below summary of data collected by the Facebook and Instagram scrapers, which Bright Data claims is publicly available:

The Facebook Scraper template, for example, only allows Bright Data's customers to scrape Facebook public data including profile name, image, handle, picture, status, shares, followers, ID, country code, region, title, views, posts, timestamp, likes, comments, groups, marketplace, members, organization, phone, address, website, etc.

The Instagram Scraper similarly only allows Bright Data's customers to scrape Instagram public data, such as followers, emails, photos, comments, name, account, avatar, business category, hashtag, followers, ID, country code, region, title, profile, views, posts, profile image, timestamp, highlights, likes, biography, business address, and average engagement.

Meta contends that “[o]n at least one occasion, Bright Data provided a third party with data from Instagram that was not, at the time, [publicly] available on Instagram.” *Id.* at ¶ 7. But this does not prove logged-in scraping. Data that was not currently publicly available on Instagram could have been publicly accessible earlier (for example, before a user updated their privacy settings). Meta provides no information about the timing of the collection of this data and the fact that it could only have been obtained by a logged-in user.

Meta places great weight on evidence that Bright Data uses tools to “circumvent Meta’s access restrictions,” such as CAPTCHAs designed to allow only human users to access the site. Meta’s Opp. at 22. Meta claims that this evidence allows a factfinder to reasonably conclude that Bright Data collected data “behind authentication barriers.” Meta’s Opp. at 22. But Meta surely understands the difference between defeating anti-automated scraping and piercing privacy walls. As this Court has noted, “using an automated program to bypass a CAPTCHA is different from accessing a password-protected site.” *hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099, 1113 (N.D. Cal. 2017) (Chen, J.) [hereinafter *hiQ I*].

Professor Kerr persuasively argues that where an individual employs an automated program that bypasses a CAPTCHA—a program designed to allow humans but to block “bots” from accessing a site—he has still not entered the website “without authorization.” Unlike a password gate, a CAPTCHA does not limit access to certain individuals; it is instead intended “as a way to slow [ ] a user’s access rather than as a way to deny authorization to access.” Other measures taken by website owners to block or limit access to bots may be thought of in the same way. A user does not “access” a computer “without authorization” by using bots, even in the face of technical countermeasures, when the data it accesses is otherwise open to the public.

*Id.* at 1113 (quoting Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1170 (2016) (alterations in original)).

Here, Meta “left the gate open” by choosing not to place all its content behind a password-protected barrier. Bright Data’s Mot. at 13. It cannot argue that circumventing Meta’s access restrictions using CAPTCHAs to block automated scraping of public information is equivalent to

---

Kol Decl. at ¶¶ 29-30.

1 scraping behind a log-in screen. The difference is pivotal, and Meta, while producing evidence of  
 2 Bright Data’s defeat of automated scraping mechanisms, has not raised a reasonable inference that  
 3 Bright Data engaged in logged-in scraping of non-public data behind a privacy wall (*e.g.*, while  
 4 logged-in).

5 The strongest evidence Meta offers from its Anti-Scraping Team’s investigation is that  
 6 Bright Data advertises one of its scraping tools—the “Scraping Browser”—as being compatible  
 7 with a program named “Puppeteer” which is “capable of automating into a website as well as  
 8 simulating many other user actions, which would allow automated collection of information  
 9 available only to users logged into Facebook or Instagram accounts.” Karumudi Decl. at ¶ 8, Exs.  
 10 A & B. However, this evidence is insufficient to raise a reasonable inference of actual logged-in  
 11 scraping by Bright Data. Mr. Karumudi’s declaration and the accompanying advertisement for  
 12 Bright Data’s Scraping Browser, *see id.* Ex. B, merely state that the product is “compatible” with  
 13 Puppeteer, not that the Scraping Browser works in the same way as Puppeteer. *Id.* Ex. B. Indeed,  
 14 Bright Data’s advertising on its website, attached to Mr. Karumudi’s declaration, makes clear that  
 15 the data scraped is publicly available data “accessible to anyone without the need to log in or enter  
 16 any password.” *Id.* Ex. A.

17 Hence, there is no disputed issue of fact on the question of logged-in scraping. Therefore,  
 18 Meta cannot meet its burden of proof to show that Bright Data scraped non-public data while  
 19 logged into a Facebook or Instagram account. Having found no disputed issue of fact that Bright  
 20 Data only engaged in logged-off scraping, the Court must now consider the legal question of  
 21 whether the Facebook and Instagram Terms should be construed to prohibit logged-off scraping of  
 22 publicly available data by Bright Data.

## 23 2. The Contract

24 Meta argues that Bright Data is bound by Facebook’s Terms sections 3.2.1, 3.2.2, 3.2.3,  
 25 and 3.2.5 and the Instagram Terms, which Meta claims prohibited Bright Data’s scraping activity  
 26 prior to and after termination of Bright Data’s accounts. Compl. at ¶ 68; Meta’s Opp. at 7-9; 17.  
 27 Bright Data responds that the Terms do not prohibit scraping publicly available data while not  
 28 logged in. Also, Bright Data contends that, after it terminated the contracts with Meta, there was

no valid contract in effect that prohibited Bright Data’s post-termination scraping activity given the fact that Bright Data manifestly rejected the Terms; nor was there any consideration for entering into a new agreement post termination.<sup>2</sup> Bright Data’s Mot. at 1-3. Bright Data also disputes whether the survival clause in section 4.2 of the Terms can render section 3 applicable to prohibit post-termination scraping.

To determine the applicability and scope of Meta’s contract Terms, the Court first examines the text of the Terms. *AIU Ins. Co. v. Superior Ct.*, 51 Cal. 3d 807, 822 (1990). The Meta Terms govern the “use” of Facebook, Messenger, and the other Products Meta offers. Compl. at ¶ 20; Munkittrick Decl. Ex 1 at 1 (preamble). However, the Instagram Terms specifically say that the Meta Terms of Service do not apply to use of Instagram. Munkittrick Decl. Ex 1 at 2. Therefore, the Facebook and Instagram Terms must be considered separately.

a. Facebook Terms

The Facebook Terms at issue are the following.

The preamble to the Terms state, “These Terms govern your use of Facebook, Messenger, and the other products . . . we offer . . .” It also states, “By using our Products, you agree that we can show you ads that we think may be relevant to you and your interests.”

Section 1 describes the services offered by Meta, including that Meta will “Provide a personalized experience for you,” “Connect you with people and organizations you care about,” “Empower you to express yourself and communicate about what matters to you,” “Help you discover content, products, and services that may interest you,” and “Ensur[e] access to our services.”

Section 2 explains that, “[i]nstead of paying to use Facebook . . . , by using the Meta Products covered by these Terms, you agree that we can show you personalized ads and other commercial and sponsored content . . .”

---

<sup>2</sup> In Bright Data’s December 4, 2022, letter to Meta claiming that Bright Data had deleted its Facebook and Instagram accounts, Bright Data stated that it “affirmatively rejects and has not consented to any agreement to your user terms in any context for any reason.” Munkittrick Decl. Ex. 4; see also Mot. at 5. This statement cannot reasonably be read to disavow retrospectively an existing contract. No contract theory supports the idea that one can retroactively terminate a pre-existing contract so as to nullify nunc pro tunc. The effect, if any, applies prospectively.

Section 3 is entitled “Your commitments to Facebook and our community,” and states that, in exchange of Meta’s provision of services, “we need you to make the following commitments.”

Section 3.1 Describes “Who can use Facebook.” It requires a user to provide for their account the same name used in everyday life, provide accurate information about themselves, create only one account the user owns, and not share their password or transfer the account to another without Meta’s permission.

Section 3.2, in its introduction, states:

We want people to use Meta Products to express themselves and to share content that is important to them, but not at the expense of the safety and well-being of others or the integrity of our community. *You therefore agree not to engage in the conduct described below (or to facilitate or support others in doing so).*

Section 3.2.1 provides that:

You may not **use** our Products to do or share anything:

That violates these Terms, the Community Standards, or other terms and policies that apply to your use of our Products.

That is unlawful, misleading, discriminatory or fraudulent (or assists someone else in using our Products in such a way).

*That you do not own or have the necessary rights to share.*

That infringes or violates someone else’s rights, including their intellectual property rights (such as by infringing another’s copyright or trademark, or distributing or selling counterfeit or pirated goods), unless an exception or limitation applies under applicable law.

Section 3.2.2 provides that:

You may not upload viruses or malicious code, use the services to send spam, or *do anything else that could disable, overburden, interfere with, or impair the proper working, integrity, operation, or appearance of our services, systems, or Products.*

Section 3.2.3 provides that:

You may not *access or collect data* from our Products *using automated means (without our prior permission) or attempt to access data you do not have permission to access.*

Section 3.2.5 provides that:

*You may not sell, license, or purchase any data obtained from us or*

our services, except as provided in the Platform Terms.

Munkittrick Decl. Ex. 1 §§ 1, 2, 3, 3.1, 3.2, 3.2.1-3.2.3, 3.2.5 (emphasis added).

b. Instagram Terms

In a similar vein, the Instagram Terms of Use say the following:

*You can't attempt to create accounts or access or collect information in unauthorized ways. This includes creating accounts or collecting information in an automated way without our express permission.*

The Instagram Terms, which are similarly structured, also prohibit, *inter alia*:

*Impersonat[ing] others or provid[ing] inaccurate information. You don't have to disclose your identity on Instagram, but you must provide us with accurate and up to date information (including registration information), which may include providing personal data. Also, you may not impersonate someone or something you aren't, and you can't create an account for someone else unless you have their express permission.*

*[D]o[ing] anything unlawful, misleading, or fraudulent or for an illegal or unauthorized purpose.*

*[V]iolat[ing] (or help[ing] or encourag[ing] others to violate) these Terms or our policies, including in particular the Instagram Community Guidelines, Meta Platform Terms and Developer Policies, and Music Guidelines.*

*[D]oing anything to interfere with or impair the intended operation of the Service[; and]*

*[S]ell[ing], licens[ing], or purchas[ing] any account or data obtained from us or our Service. This includes attempts to buy, sell, or transfer any aspect of your account (including your username); solicit, collect, or use login credentials or badges of other users; or request or collect Instagram usernames, passwords, or misappropriate access tokens.*

Munkittrick Decl. Ex. 2 (emphasis added).

3. Bright Data was bound by Meta's Terms while it had Facebook and Instagram accounts

Bright Data concedes that, while it had accounts with Facebook and Instagram between April 1, 2022, and December 4, 2022, it was bound by the Facebook and Instagram Terms.

Holtzblatt Decl. Ex. D at 8.<sup>3</sup> Bright Data does not contest that “[a]ll Facebook and Instagram

<sup>3</sup> The Court notes that a visitor to Facebook and Instagram could access Facebook or Instagram

users must agree to the Facebook and Instagram Terms.” Compl. at ¶ 77; *accord Meta Platforms, Inc. v. BrandTotal Ltd.*, 605 F. Supp. 3d 1218, 1257 (N.D. Cal. 2022) (Spero, J.) (“[A]ll users who create accounts indicate that they agree to Meta’s terms of use.”). However, Bright Data claims it did not violate the Terms because the Terms do not apply to its activity of scraping data while it is not logged in to Facebook or Instagram. In particular, Bright Data argues that the Terms govern the “use” of Facebook and Instagram but that its scraping of public data while logged out does not constitute “use” governed by the Terms. Bright Data’s Mot. at 20. Therefore, the Court must analyze whether the Terms, properly construed, bar Bright Data’s logged-off automated scraping of publicly available data.

4. Bright Data’s logged-off scraping and sale of data does not violate the Facebook and Instagram Terms

Meta argues that both logged-on and logged-off conduct is covered by the Terms and therefore Bright Data’s actions violate the Facebook and Instagram Terms. Meta’s Opp. at 17. Bright Data responds that its logged-off scraping of public data is not covered by the Terms because it is not a “user” of Facebook or Instagram when engaged in such activity. Bright Data’s Mot. at 20.

a. Canons of contract interpretation

The Court applies California law in interpreting the Terms. The Terms recite that California law applies, *see, e.g.*, Bright Data’s Mot., Ex. 1 (Facebook Terms § 4.4) (providing that “the laws of the State of California will govern these Terms and any claim, cause of action, or dispute without regard to conflict of law provisions”); *id.*, Ex. 2 (Instagram Terms) (providing for the same in the subsection titled “How We Will Handle Disputes”), and, as reflected in their papers, the parties have proceeded with that understanding. *See also* Cal. Civ. Code § 1646 (“A

---

without ever having read the Terms. However, in order to create an account, one must click through the “Create new account” and the “Sign up” screens (Facebook) or click the “Sign up” button (Instagram) and enter their account information to view and agree to the Terms. Even after following these steps, someone creating an account is not required to click “accept” in order to agree to the Terms. The Terms are hyperlinked on the “Create new account” (Facebook) and “Sign up” (Instagram) screen and users are informed that by proceeding further and creating an account, they are agreeing to the Terms. Therefore, an account holder could create and use an account without ever having read the Terms. *See* <https://www.facebook.com/>; <https://www.instagram.com/>.

contract is to be interpreted according to the law and usage of the place where it is to be performed; or, if it does not indicate a place of performance, according to the law and usage of the place where it is made.”); *Johnson v. Walmart Inc.*, 57 F.4th 677, 681 (9th Cir. 2023); *accord Glob. Commodities Trading Grp., Inc. v. Beneficio de Arroz Choloma, S.A.*, 972 F.3d 1101, 1111 (9th Cir. 2020). “Under California law, contract interpretation is a question of law.” *In re Bennett*, 298 F.3d 1059, 1064 (9th Cir. 2002); *S. California Stroke Rehab. Assocs., Inc. v. Nautilus, Inc.*, 782 F. Supp. 2d 1096, 1110 (S.D. Cal. 2011) (citing *SDR Capital Mgmt., Inc. v. Am. Int’l Specialty Ins. Co.*, 320 F. Supp. 2d 1043, 1046 (S.D. Cal. 2004)); *see also Parsons v. Bristol Develop. Co.*, 62 Cal.2d 861 (1965).

Interpretation, starts, of course, with the text of the contract. When interpreting a contract, the mutual intention of the parties is normally discerned “from the written terms [of the contract] alone,” so long as the “contract language is clear and explicit and does not lead to absurd results.” *Kashmiri v. Regents of Univ. of Cal.*, 156 Cal. App. 4th 809, 831 (2007); *see also Revitch v. DIRECTV, LLC*, 977 F.3d 713, 717 (9th Cir. 2020); *AIU Ins.*, 51 Cal. 3d at 822 (“if the meaning a layperson would ascribe to contract language is not ambiguous, [courts must] apply that meaning”); *ASP Props. Grp., L.P. v. Fard, Inc.*, 133 Cal. App. 4th 1257, 1269 (2005) (contract interpretations must be fair and reasonable and must not lead to “absurd” results) (internal quotation marks omitted). “A primary rule of interpretation is that “[t]he common or normal meaning of language will be given to the words of a contract unless circumstances show that in a particular case a special meaning should be attached to it.” *Hunt Wesson Foods, Inc. v. Supreme Oil Co.*, 817 F.2d 75, 77 (9th Cir. 1987) (quoting 4 Samuel Williston & Richard A. Lord, A Treatise on the Law of Contracts § 618 (3d ed. 1961) [hereinafter Williston on Contracts]).

Further, “[a] written contract must be read as a whole and every part interpreted with reference to the whole, with preference given to reasonable interpretations.” *Pauma Band of Luiseno Mission Indians of Pauma & Yuima Rsrv. v. California*, 813 F.3d 1155, 1170 (9th Cir. 2015); *accord Joseph v. City of Atwater*, 74 Cal. App. 5th 974, 983 (2022) (stating that under California law, “reading a sentence in isolation is not reasonable because California law requires contracts to be interpreted as a whole”). “An interpretation which gives effect to all provisions of

1 the contract is preferred to one which renders part of the writing superfluous, useless or  
2 inexplicable.” *Pauma*, 813 F.3d at 1171 (internal quotation marks omitted).

3 On the other hand, if there is sufficient ambiguity such that the contract is “reasonably  
4 susceptible” to either of the two interpretations urged by the parties, extrinsic evidence may be  
5 offered to prove either of these meanings is admissible. *Id.* at 40 (internal citations omitted). As  
6 such, extrinsic evidence may be used in contract interpretation when the contract’s terms are  
7 ambiguous; indeed, under California law, extrinsic evidence may be used to establish a contract  
8 term is in fact ambiguous. *Pac. Gas & Elec. Co. v. G.W. Thomas Drayage & Rigging Co., Inc.*,  
9 69 Cal. 2d 33, 40 n.8 (1968); *accord Ewert v. eBay, Inc.*, Nos. C-07-02198, C-07-04487, 2010 WL  
10 4269259, at \*6-7 (N.D. Cal. Oct. 25, 2010); *Abifadel v. Cigna Ins. Co.*, 8 Cal. App. 4th 145, 159  
11 (1992).

12 Moreover, the court must consider “all credible evidence offered to prove the intention of  
13 the parties,” including evidence of the circumstances surrounding the formation of the agreement  
14 such as the “object, nature, and subject matter of the writing.” *Pac. Gas & Elec.*, 69 Cal. 2d at 39-  
15 40; *accord* 11 Williston on Contracts § 32:7; *Milenbach v. C.I.R.*, 318 F.3d 924 (9th Cir. 2003)  
16 (applying California law); *La Jolla Beach & Tennis Club, Inc. v. Indus. Indem. Co.*, 9 Cal. 4th 27  
17 (1994), *as modified on other grounds* (Mar. 2, 1995). These surrounding circumstances refer to  
18 “the commercial or other setting in which the contract was negotiated and other objectively  
19 determinable factors that give a context to the transaction between the parties.” *Id.* Such  
20 surrounding circumstances may be considered notwithstanding the parol evidence rule; they may  
21 be admitted even if the contract Terms are not ambiguous. *Id.*; *accord Milenbach v. C.I.R.*, 318  
22 F.3d at 924.

23 Finally, when other rules of interpretation do not resolve an apparent ambiguity, courts  
24 resolve ambiguities in contract language against the drafter. *ASP*, 133 Cal. App. 4th at 1269;  
25 *accord Victoria v. Superior Ct.*, 40 Cal. 3d 734, 739 (1985); *Sandquist v. Lebo Auto., Inc.*, 1 Cal.  
26 5th 233, 248 (2016). “[T]he rule requiring the resolution of ambiguities against the drafting party  
27 applies with peculiar force in the case of a contract of adhesion. Here the party of superior  
28 bargaining power not only prescribes the words of the instrument but the party who subscribes to

it lacks the economic strength to change such language.” *Sandquist*, 1 Cal. 5th at 248 (cleaned up). “In cases of doubt, therefore, so long as other factors are not decisive, there is substantial reason for preferring the meaning of the [non-drafting] party.” Restatement (Second) of Contracts [hereinafter Rest. 2d], § 206, cmt. a. Again, this is especially true where, as here, the contract is one of adhesion. *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 793-94 (N.D. Cal. 2022) (Orrick, J.) (“Meta’s terms must have only one plausible interpretation” in order for that construction to be deemed the correct one). Meta does not dispute that the Terms are a standardized contract of adhesion. Meta’s Opp. at 13.

b. Bright Data did not “use” Facebook or Instagram when it engaged in logged-off scraping of public data

The Terms provide that they govern “your use” of, *e.g.*, Facebook and Instagram.<sup>4</sup> It is reasonable to interpret the Terms such that Bright Data did not “use” Facebook and Instagram when it engaged in public logged-off data scraping. When subjected to established canons of construction, the Facebook and Instagram Terms support the interpretation that the Terms only prohibit logged-in scraping, and not logged-off scraping.

There are two requirements to the “use” of Facebook and Instagram. First, one must be a user—meaning someone with an active account.<sup>5</sup> Second, one must engage in a covered “use” of Facebook and Instagram.

i. A “user” of Facebook and Instagram is one who has an active account

Mere visitors without a Facebook or Instagram account do not see the Terms and are not

---

<sup>4</sup> The Meta Terms of Service expressly do not apply to Instagram.

<sup>5</sup> Although the Terms more commonly refer to “use” rather than “user,” the Terms do use the term “user.” See, *e.g.*, Bright Data’s Mot., Ex. 1 (Facebook Terms § 1) (addressing, *inter alia*, safety and security of “our community of users” as well as “ways to make our services better” which “includes analyzing data we have about our users”); *id.* (Facebook Terms § 2) (referring to “usernames”); *id.* (Facebook Terms § 3.1) (referring to “content that you create collectively with other users”); Bright Data’s Mot., Ex. 2 (Instagram Terms, section titled “Your Commitments”) (stating that “[y]ou can’t sell, license, or purchase any account or data obtained from us or our Service” which “includes attempts to buy, sell, or transfer any aspect of your account (including your username); solicit, collect, or use login credentials or badges of other users; or request or collect Instagram usernames, passwords, or misappropriate access tokens”). Obviously, one who “uses” Facebook or Instagram is a “user.”

asked to consent to them. In fact, they cannot even see the Terms until they begin the signup process for a Facebook or Instagram account and enter their information. At that point, the Terms are hyperlinked on the signup screen with accompanying text that tells users that by proceeding further and creating an account, they agree to the Terms.<sup>6</sup> Without going through this process, a visitor would not even have the opportunity to see the Terms, nor could the visitor consent to the Terms. This indicates that a visitor is not a “user” of Facebook or Instagram who can be bound by the Terms; rather, a user is someone who has a Facebook or Instagram account.

That a non-subscribing visitor is not a “user” bound by the Terms is underscored by a change that was made to the Facebook Terms. The 2009 Facebook Terms included the following clause: “accessing or using our website . . . signif[i]es that you . . . agree to be bound by these Terms . . . , whether or not you are a registered member of Facebook.” Meta’s Opp. at 18 (quoting the 2009 version of the Terms at issue in *Fteja v. Facebook, Inc.*, 841 F. Supp. 2d 829, 839-841 (S.D.N.Y. 2012), Docket No. 6-1 (Apr. 4, 2011)) (emphasis in original). That clause has since been removed, *i.e.*, is not in the current Terms. The now-obsolete clause demonstrates that Meta was fully aware of how to write a clear provision that applied to both logged-in and logged-off users and made a conscious decision not to include the distinction in the most recent iteration of the Terms for Facebook and Instagram. Therefore, it is reasonable to infer that the current Terms contemplate a “user” as an account holder.

Moreover, the text of the Terms underscores the reasonable interpretation that a “user” of Facebook and Instagram bound by their Terms is one with an active account. Section 3 provides that a user of Facebook must make a range of “commitments” in exchange for Meta’s provision of services, Munkittrick Decl. Ex. 1 § 3 (emphasis added), all of which require an account. Section 3.1 is titled “Who can use Facebook.” Its stipulations contemplate that only those with accounts are users: The user must ensure their “account” name and personal information is accurate; use only one account and use it only for personal purposes; and refrain from sharing their password, giving access to their account to others, or transferring their account to someone else without

---

<sup>6</sup> See <https://www.facebook.com/>; <https://www.instagram.com/>.

Meta’s permission. *Id.* § 3.1 (emphasis added). The Instagram Terms raise the same inference. Under a heading outlining user “commitments,” the subsection “Who Can Use Instagram” states that a user cannot have previously had “*your account*” disabled. *Id.* Ex. 2.

The language of the Terms regarding prohibited activities on Facebook and Instagram also supports the interpretation that a user is an active account holder. Section 3.2 is entitled, “What you can share and do *on Meta Products*.” Munkittrick Decl. Ex. 1 § 3.2 (emphasis added). The Instagram Terms also discuss what users can and can’t do “*on Instagram*.” *Id.* Ex. 2. This language, too, contemplates users as active account holders. A mere visitor could not be “on” Facebook. And, the prohibited activities “on Instagram” include “impersonat[ing] others or provid[ing] inaccurate information,” including “*registration information*”; “buy[ing], sell[ing], or transfer[ing] any aspect of *your account*”; “solicit[ing], collect[ing], or us[ing] *login credentials* or badges of other users”; or “*request[ing] or collect[ing] Instagram usernames, passwords, or misappropriate[ing] access tokens*,” *id.*—all activities unique to account holders. “Use” of Facebook and Instagram means action taken by logged-in users by account holders

- ii. “Use” as contemplated by the Terms reasonably refers to action taken by account holders (users) while they are logged in

The preamble and sections 1 and 2 of the Facebook Terms, as well as related sections of the Instagram Terms, support the interpretation that “use” of Facebook and Instagram is conduct undertaken while logged into an account. The preamble and section 1 of the Meta Terms state that by “using” Meta’s Products, users agree that Meta can show them “personalized” ads and that using Facebook is a “personalized experience” that is “unlike anyone else’s.” Munkittrick Decl. Ex. 1 preamble, § 1. Section 1 describes the products and services Meta provides—the “personalized experience” available when the user signs in. *Id.* § 1. Without logging into an account, Meta could not collect data on “the connections you make, the choices and settings you select, and what you share and do on and off [its] Products” in order to “personalize your experience.” *Id.* Without an account holder who logs in, Meta could not “help you find and connect with people, groups, businesses, and others that matter to you across the Meta Products you use.” *Id.* And without an account holder who logs in, a user could not “express yourself on

Facebook to communicate with friends, family, and others about what matter to you.” *Id.* Facebook purports to provide these unique “services” that differ from anyone else’s experience by varying “the posts, stories, events, ads, and other content you see”; making suggestions for “groups to join, events to attend, Facebook pages to follow or send a message to, shows to watch, and people you may want to become friends with”; “connecting you with people and organizations you care about”; and allowing users to express themselves by posting, “liking” other people’s posts, or sharing photos. *Id.* Ex. 1 § 1. All these activities require log-in.

The same is true of the Instagram Terms. Because “[p]eople are different,” Instagram claims that it offers “personalized opportunities” for users to “create, connect, communicate, discover and share.” *Id.* Ex. 2. Without an account and log-in, how could Instagram create such a personalized experience “based on things that you and others do on and off Instagram,” enable its users to “grow [their] presence,” “strengthen [their] relationships through shared [online] experiences,” and “communicate with people” on Instagram? *Id.* Ex. 2. The language of the Terms speaks to the unique experience of every individual, adding to the reasonable interpretation that the Terms contemplate “users” as those with accounts and “use” as activity while logged into those accounts.

Moreover, the funding structure of Facebook and Instagram supports the reasonable interpretation that one cannot “use” Facebook without logging into an account. Section 2 of the Facebook Terms states that instead of paying to “use” Facebook, the user agrees that Facebook can show the user personalized ads and other commercial and sponsored content for which Facebook is paid. The basic financial model depends on account holders logging in; otherwise, they do not see ads and Facebook does not get paid. As for Instagram, the Terms say that they will use data from Instagram and other Meta products to “show you ads, offers, and other sponsored content that . . . [are] meaningful to you.” *Id.* § 2. Under the heading “How Our Service Is Funded,” the Instagram Terms state that they receive payment through ads that they show to users. *Id.* Without a user logging in to see these ads, Instagram cannot receive funding.

Finally, similar to visitors to a news website who read a “free article that news websites sometimes offer before redirecting readers to a paywall” would not be able to make “use” of the

1 full functions of the site, see Meta’s Mot. at 16, there is a reasonable inference that visitors to  
2 Facebook and Instagram, who do not have accounts, could not “use” the site because the logout  
3 mechanism and other technological restrictions would prevent them from doing so.

4 c. Bright Data’s logged-out scraping is unrelated to the purpose of its accounts

5 The fact that Bright Data had Facebook and Instagram accounts when it scraped is entirely  
6 incidental and unrelated to its scraping. There is no evidence that Bright Data used the accounts or  
7 any information from the accounts to facilitate scraping of publicly accessible data. It is not  
8 disputed that Bright Data maintained the accounts for an entirely collateral purpose—to engage in  
9 its own advertising on Facebook and Instagram—which was unrelated to its scraping of public  
10 data. When Bright Data scraped data, it did so without logging in and using its Meta accounts;  
11 instead, it was acting in the exact same capacity as any outside non-subscribing visitor trying to  
12 overcome Meta’s anti-bot technology. Therefore, even though Bright Data could technically be  
13 characterized as a “user” of Facebook and Instagram inasmuch as it maintained accounts on those  
14 platforms, there is a strong and compelling argument that Bright Data was not “using” Facebook  
15 as contemplated by the Terms when it scraped public data while not logged-in.

16 d. The Terms could arguably support an alternative construction of “use” and  
17 “user”

18 To be sure, some aspects of the Facebook and Instagram Terms could support a  
19 construction under which one could “use” Facebook and Instagram without logging into an  
20 account.

21 Although the Meta Terms of Service, section 3.2, begin “You may not *use* our Products ”  
22 to violate the Terms, some subsequent sections list violations which do not mention or necessarily  
23 require logging in. *Id.* § 3.2.1. For instance, section 3.2.2 prohibits interference with Meta’s  
24 systems or Products, while section 3.2.3 simply prohibits “access” or “collect[ion]” of data from  
25 Meta “using automated means (without [Meta’s] prior permission),” and section 3.2.5 prohibits  
26 “sell[ing], licens[ing], or purchas[ing] data obtained from Meta or its services. *Id.* §§ 3.2, 3.21-  
27 3.23, 3.25. Similarly, the language of the Instagram Terms does not explicitly limit the  
28 Instagram’s prohibitions to activities that must be conducted with an account. Although many of

the prohibited activities are unique to account holders, some, like impersonating others, collecting Instagram usernames, and collecting login credentials (which are not limited to a username and password but could include other identifiers to assist with login) are not explicitly limited to those with accounts. In fact, Bright Data’s Chief Technology and Security Officer attests that account usernames and other account identifier credentials are part of the “public” data Bright Data accesses without logging in. Kol Decl. at ¶¶ 29-30.

On the other hand, those prohibitions could reasonably be interpreted as applying to activities tied to or derivative of logged-in access, such as the selling of data which had been obtained while the user was logged in. In this regard, Bright Data notes that section 3.2.3 of the Facebook Terms is ambiguous because it prohibits automated data collection and access without Meta’s permission. Bright Data’s Mot. at 22. That section states: “You may not *access or collect data* from our Products using *automated* means (*without our prior permission*) . . .” Munkittrick Decl. Ex. 1 § 3.2.3 (emphasis added). In Bright Data’s view, the “only reasonable interpretation” of “unauthorized” or “without our prior permission” is that Meta’s “authorization” comes through a user account; “authorization” under the Terms need not be obtained by those who have no such account. *Id.* Otherwise, says Bright Data, Meta’s interpretation would lead to the absurd result that “all public web search (including manual visitation) [would be] ‘unauthorized.’” *Id.*

Meta nonetheless argues that the Terms’ language pertaining to unauthorized automated access, collection, and sale of data support a broad interpretation of “user.” Meta contends that “any user that *visits* Facebook uses Facebook’s physical infrastructure by sending a request to Meta’s servers.” *Id.* (citing Karumudi Decl. at ¶ 4) (emphasis added). As for the Instagram Terms, Meta focuses on the portion of the Terms that provides: “When you create an Instagram account *or use* Instagram, you agree to these terms.” Munkittrick Decl. Ex. 2 (emphasis added). If “use” were interpreted as synonymous with account activity, it would be superfluous to add a distinction in the same sentence that those who have created accounts *or used* those accounts agree to the Terms. On the other hand, Bright Data contends it is reasonable to construe the word “create” as referring to people who create an account in the first instance, and “use” as referring to those who make use of the account thereafter. And the clause in the Instagram Terms that selling

1 data “includes” various prohibited activities, most of which require an account, raises an inference  
2 that the prohibition on data sale is connected to the subsequent prohibitions that require an  
3 account, and thus supports the distinction between creation and use of accounts.

4 e. The Terms are construed to not apply to scraping of public data while  
5 logged off

6 While both parties advance reasonable arguments favoring their respective construction of  
7 the Terms, the Court concludes the Terms do not apply to and prohibit Bright Data’s scraping of  
8 publicly available data while logged off. It finds Bright Data’s interpretation more convincing  
9 because it is consistent with the overall language and purpose of the user provisions of the Terms,  
10 is supported by extrinsic evidence, and comports with the canon of construction that ambiguous  
11 terms should be construed against the drafter, especially where there is an adhesion contract.

12 i. The text and intent of the parties

13 A contract should be construed in accordance with the text and intent of the parties. *See*  
14 *Foxcroft Prods., Inc. v. Universal City Studios LLC*, 76 Cal. App. 5th 1119, 1130 (2022). As  
15 discussed above, there are reasonable textual arguments advanced by Meta and Bright Data. The  
16 Court finds Bright Data’s construction more persuasive for the reasons discussed above in Part  
17 III.A.4.b-d.

18 The Court also finds Bright Data’s construction consistent with the overall purpose of the  
19 Section 3 of the Meta Terms) which can be discerned from its structure and language—the  
20 overarching purpose of the section (as informed by the Preamble and Sections 1 and 2) is to  
21 prevent account holders who have privileges and access to Meta services from abusing their access  
22 to such services. When an entity does not utilize that access to, *e.g.*, scrape public data, it does not  
23 abuse that access; it stands in the same shoes as a visitor to whom the Terms cannot apply as a  
24 matter of basic contract law. Bright Data’s account with Meta for its own marketing (and not data  
25 gathering) purposes is wholly incidental to its scraping activities. To read the Terms to apply to  
26 that incidental activity that is unrelated to their accounts stretches its application beyond its  
27 purpose, especially considering those who do not subscribe to Meta services do not see the Terms  
28 and cannot be bound thereby.

ii. Extrinsic evidence

“Whether language in a contract is ambiguous is a question of law to be answered by the court.” *Coremetrics, Inc. v. Atomic Park.com, LLC*, No. C-04-0222, 2005 WL 3310093, at \*3 (N.D. Cal. Dec. 7, 2005) (Chen, J.); *accord Abifadel*, 8 Cal. App. 4th at 159. When contractual Terms are ambiguous, extrinsic evidence is admissible to assist in resolving the ambiguity and the court must consider all credible evidence to determine the intent of the contracting parties. *Pac. Gas & Elec. Co.*, 69 Cal. 2d at 39, 40 n.8; *accord Abifadel*, 8 Cal. App. 4th at 159. The standard for admitting extrinsic evidence under California law is the following:

First, the court provisionally receives (without actually admitting) all credible evidence concerning the parties’ intentions to determine “ambiguity,” whether the language is “reasonably susceptible” to the interpretation urged by a party. If in light of the extrinsic evidence the court decides the language is “reasonably susceptible” to the interpretation urged, the extrinsic evidence is then admitted to aid in the second step interpreting the contract.

*hiQ Labs, Inc. v. LinkedIn Corp.*, 639 F. Supp. 3d 944, 960 (N.D. Cal. 2022) (Chen, J.) [hereinafter *hiQ II*] (citing *Winet v. Price*, 4 Cal. App. 4th 1159, 1165 (1992)). “The threshold issue of whether the parol evidence is necessary to determine the meaning of the language is a question of law.” *Id.* Similarly, “when the parol evidence is not conflicting, construction of the contract is a question of law.” *Id.*

Meta does not offer extrinsic evidence to support its interpretation of the Terms or to counter Bright Data’s interpretation; rather, it argues that the language of the Terms is not ambiguous at all. Docket No. 137 (“Meta’s Sur-Reply”) at 5. It also argues that precedent does not allow Bright Data to rely on extrinsic evidence to “negate or diminish” the unambiguous Terms of the contract. Meta’s Mot. at 5 (citing *hiQ II*, 639 F. Supp. 3d at 961). Meta’s argument is inapposite.

As noted above, the critical terms of the Terms are reasonably susceptible to conflicting interpretations. There is sufficient ambiguity to admit extrinsic evidence.

Bright Data offers several pieces of extrinsic evidence to support its interpretation that the Facebook Terms only bar logged-in automated scraping by account holders. First, Bright Data

offers evidence to show that a “user” must be an account holder: as noted above, the 2009 version of the Terms expressly applied to website *visitors*. Meta’s Opp. at 18. The removal of the provisions contrasting “access” to Facebook with “use” of Facebook and distinguishing registered members of Facebook from non-members indicates that Meta no longer considers mere visitors to be users of Facebook. This supports the notion that the key to “use” is the employment of a user’s privileged access when they log in.

Bright Data also offers extrinsic evidence from a 2009 declaration by a Facebook employee in a different case that also concerned an “outdated” version of the Facebook Terms. Munkittrick Decl. Ex. 11 ¶ 2; Docket No. 114 (“Bright Data’s Reply”) at 14. The declaration reads: “A putative Facebook user cannot become an actual Facebook user unless and until they have clicked through the registration page where they acknowledge they have read and agreed to Facebook’s terms of use.” Munkittrick Decl. Ex. 11 ¶ 2; Bright Data’s Reply at 14.

Lastly, Bright Data points to language from the Facebook Help Center: “You have to create a Facebook account in order to use Facebook.” Docket No. 114-1 (“Munkittrick Decl. II”) Ex. 13 at 1. Again, this supports the narrower construction of user and hence “use.”

To be sure, as Meta states, neither the declaration nor the page from the Facebook Help Center pertain directly to the Instagram Terms. Meta’s Mot. at 5. But extrinsic evidence need not be limited to the written Terms of the Instagram contract to be relevant. *Pac. Gas & Electric Co.*, 69 Cal. 2d at 39-40. That evidence is relevant inasmuch as for Instagram, like Facebook, is a Meta Product, *see* Munkittrick Decl. Ex. 2, and thus it sheds light on the overall intent of the parties at bar.

Contrary to Meta’s assertion, *see* Meta’s Sur-Reply at 5, the extrinsic evidence is not offered for a prohibited purpose to “negate or diminish” or “add to, detract from, or vary” the written Terms. *Pac. Gas & Electric Co.*, 69 Cal. 2d at 39; *accord hiQ II*, 639 F. Supp. 3d at 961. This evidence clearly speaks to the “object, nature, and subject matter” of the writing. *Pac. Gas & Electric Co.*, 69 Cal.2d at 40. It is offered to clarify terms which the Court finds ambiguous.

### iii. Canons of construction

Finally, to the extent ambiguity remains after considering the text and structure of the

Terms, its purpose and extrinsic evidence, the Court must construe any remaining ambiguity in Meta's contract against Meta, the drafter. *Victoria v. Superior Ct.*, 40 Cal. 3d at 739. As noted above, this is particularly so given the Terms is a standardized contract of adhesion. *Sandquist*, 1 Cal. 5th at 248 (“[T]he rule requiring the resolution of ambiguities against the drafting party applies with peculiar force in the case of a contract of adhesion.”) (cleaned up).

iv. Conclusion

For the reasons stated above, the Terms do not apply to Bright Data's logged-off scraping of publicly viewable data. Therefore, Meta's motion for summary judgment must be **DENIED** on this question.

f. The Facebook and Instagram Terms do not operate to bar logged-off scraping after termination

Even if the Meta, Facebook, and Instagram Terms were construed to prohibit users from scraping public data while logged off, for reasons set forth below, that prohibition would not apply to Bright Data after it terminated its Meta accounts. As to the Facebook Terms, resolution of that question turns on the interpretation and enforceability of the survival clause in section 4.2 of the Terms as to logged-off scraping. As to the Instagram Terms which contains no survival clause, the question turns on whether any post-termination ban applies at all.

i. Interpretation of the Facebook survival clause

The survival clause in the Facebook Terms states that, “[i]f you delete or we disable or delete your account, these Terms shall terminate as an agreement between you and us, but the following provisions will *remain in place*: 3, 4.2-4.5.” Munkittrick Decl. Ex. 1 § 4.2 (emphasis added). The survival clause does not specify a time limitation for those provisions remaining in place.

At the outset, the Court notes that, in addition to the general rules of contract construction which start with a focus on the text of the provision in question and include construing unresolved ambiguities against the drafted, especially with contracts of adhesion, the survival clause is subject to an additional rule of construction. Courts disfavor the application of a survival clause which purport to extend in perpetuity. The U.S. Supreme Court has advised that courts “should not

construe ambiguous writings to create lifetime promises.” *M & G Polymers USA, LLC v. Tackett*, 574 U.S. 427, 441-42, 135 S. Ct. 926, 190 L. Ed. 2d 809 (2015) (cited in Bright Data’s Mot. at 3, 24); *see also* 3 A. Corbin, Corbin on Contracts § 553, at 216 (1960). California courts have applied this presumption against perpetual agreements to various contexts, holding, for instance, in real estate contexts that “[a] construction conferring a right in perpetuity will be avoided unless compelled by the unequivocal language of the contract.” *Nissen v. Stovall-Wilcoxson Co.*, 120 Cal. App. 2d 316, 319 (1953) (invalidating trial court’s interpretation of land purchase agreement as binding the defendant to pay all land assessments without time limitations). For this reason, courts generally hold that, for a survival clause to be valid and enforceable, the clause must be limited in scope as to its geography and duration. *See, e.g., Nalco Chem. Co. v. Hydro Techs., Inc.*, 984 F.2d 801, 804 (7th Cir. 1993). Courts have invalidated or limited the scope of perpetuity provisions in other contexts as well. *See Nissen*, 120 Cal. App. 2d at 319; *Foster Cable Servs., Inc. v. Deville*, 368 F. Supp. 3d 1265, 1274 (W.D. Ark. 2019) (stating that “[t]he fact that the [confidentiality] Agreement does not state a time limitation, but instead applies forever, further supports a finding that it is unenforceable”); *Howard Schultz & Assocs. v. Broniec*, 239 Ga. 181, 187 (1977) (finding that a nondisclosure covenant with “no time limitation” was therefore “unenforceable”); *Nalco*, 984 F.2d at 804 (determining that a confidentiality clause without “a durational limitation” was void and unenforceable, except as to trade secret restrictions). Survival clauses are generally limited to “conduct that arises out of or shares a nexus to,” the agreement. *Nolde Bros.*, 430 U.S. at 249.

Bright Data argues for a narrow construction of the survival clause. Bright Data contends that the survival clause only preserves bans on logged-in scraping conduct in which a user engaged *pre-termination* and post-termination conduct *arising out of* that pre-termination activity. *See* Bright Data’s Reply at 10-11; *see also* Bright Data’s Mot. at 25. The survival clause was intended to “address enforcement of claims arising from pre-termination conduct, not to create lifetime bans for conduct unrelated to parties’ contractual relationship.” Bright Data’s Reply at 10-11; *see also* Bright Data’s Mot. at 25. This construction, Bright Data argues, allows Meta to “assert an independent breach for post-termination sale of Facebook data collected *pre-*

1 *termination.*” *Id.* “Bright Data does not dispute that the survival clause preserves claims arising  
 2 out of pre-termination use of a user account. [It argues] only that post-termination conduct that  
 3 does not make use of any such account is not covered.” Bright Data’s Mot. at 28. For instance, if  
 4 Bright Data unlawfully scraped data during the contract period, the survival clause permits Meta  
 5 to sue for the breach after termination of the account; it would also permit Meta to sue Bright Data  
 6 for post-termination sale of data wrongfully collected pre-termination. It would not, however, bar  
 7 conduct engaged in entirely after termination, including post-termination scraping.

8 Meta, on the other hand, contends that the Terms impose continuing obligations with  
 9 respect prohibited scraping, even that which occurs entirely after termination of Meta accounts.  
 10 Meta’s Opp. at 11. Otherwise, says Meta, a user “could create accounts, use them for scraping,  
 11 and then seek to evade liability by cancelling their accounts.” Munkittrick Decl. Ex. 8 at 12;  
 12 Bright Data’s Mot. at 28. (The Court notes that Meta does not explain how Bright Data used its  
 13 Meta account for scraping if it only scraped public data while logged off.) Meta adds that the  
 14 survival clause “without a defined expiration” is “vital to Meta’s ability to protect its users’ data  
 15 and enforce the Facebook Terms” and that it “ensures . . . that [Meta] can terminate an account  
 16 and still be able to enforce the Terms.” Meta’s Opp. at 11. Under Meta’s interpretation, the  
 17 Terms’ prohibition on automated scraping is effective in perpetuity.

18 Bright Data’s interpretation of the survival clause of section 4.2 is persuasive for several  
 19 reasons. First, Meta’s broad interpretation of the clause runs counter to the disfavoring of contract  
 20 restrictions that appear to apply in perpetuity as held in the above cited cases. Restricting the  
 21 scope of the survival clause to enforcement of Meta’s rights with respect to Bright Data’s pre-  
 22 termination conduct assures that the clause applies only to “conduct that arises out of or shares a  
 23 nexus to,” the agreement which as noted above focuses on users (i.e. those with active accounts).  
 24 *Nolde Bros.*, 430 U.S. at 249. The disfavoring of Meta’s broad interpretation of section 4.2 is  
 25 amplified by policy concerns here which concern access to the Internet. *See hiQ I*, 273 F. Supp.  
 26 3d at 1112. *Cf. Packingham*, 582 U.S. 98 at 107-08 (emphasizing First Amendment interest in  
 27 maintaining accessibility of the Internet as an open forum). As the Ninth Circuit warned in *hiQ*:

28 “Giving companies like [Meta] 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 III*, 31 F.4th at 1202.

Second, Bright Data’s interpretation is consistent with the structure of the Terms. Notably, section 4.2 (of which the survival clause is a part) addresses the key enforcement mechanism of “Account suspension or termination.” It addresses enforcement rights of Meta. The survival clause insures that certain procedural rights and protections survive—such as the limits on Meta’s liability (section 4.3), Meta’s choice of law and venue (section 4.4), the integration clause (section 4.5.1), the severance clause (section 4.5.3), and restrictions on third party beneficiary rights (section 4.5.6)—rights and protection that one would naturally expect to survive contract termination. Munkittrick Decl. Ex. 1 §§ 4.2-4.5. As to the survival clause’s reference to section 3, there are numerous provisions within Section 3 that naturally warrant survival. For instance, section 3.3, titled “The permissions you give us,” stipulates users give Meta “license” to “store, copy, and share [user content] with others,” *see* Munkittrick Decl. Ex. 1 § 3.3.1; the right to use the user’s “name, profile picture, and information about [their] actions [in connection] with ads and sponsored or commercial content,” *see id.* § 3.3.2; and the right to update software that users have downloaded, *see id.* § 3.3.3. Section 3.4 provides for Meta’s continued control over its intellectual property such as its copyrights, trademarks, and source code. *Id.* § 3.4. These are matter which naturally need to survive in order for Meta to control its legally protectible intellectual property rights. The structure of the Terms thus supports Bright Data’s construction of the survival clause as “an enforcement mechanism, not an independent creator of lifetime bans.” Bright Data’s Reply at 11. *See also Am. Nat’l Ins. Co. v. Akopyan*, No. 22-55208, 2023 WL 2203554, at \*2 (9th Cir. 2023) (interpreting a clause narrowly based on its location and “surround[ing]” provisions in the contract).

Further, as Bright Data notes, the “remain in place” fragment of the survival clause does *not* appear in the section titled “Your commitments to Facebook and our community,” which describe the user’s obligations to refrain from engaging in activities prohibited by the Terms. Munkittrick Decl. Ex. 1 § 3. That “commitments” section (section 3) contains its own remedy

provision, outlined in subsection 3.2 which provides for account termination. Munkittrick Decl. Ex. 1 § 3.2 (“We can remove or restrict access to content . . . [or] suspend or disable your account.”). The enforcement language in section 3.2 does not contain a survival clause even though that would seem to be a natural place to insert such a provision if it was so intended.

Third, the language of the survival clause which states, “the following provisions will remain in place: 3, 4.2-4.5” itself is not without ambiguity. The term “remain in place” is less than precise. Moreover, the clause refers to the entirety of section 3. Yet, section 3 is lengthy and multifaceted and contain provisions which clearly have no applicability after termination of an account. *See, e.g.*, section 3.1 (“Who can use Facebook”), section 3.2 (pertaining to Meta’s right to terminate or suspend accounts). As noted above, ambiguities are to be construed against the drafter of an adhesion contract—Meta. Fourth, Meta’s broad construction of the survival clause could lead to absurd results. *See Kashmiri v. Regents of Univ. of Cal.*, 156 Cal. App. 4th 809, 831 (2007) (contract should not be construed to lead to absurd results). As Bright Data states, “[n]o reasonable person reading the Facebook Terms would believe that the four-word fragment—‘will remain in place’—forever strips them of their lawful right to search the web.” Bright Data’s Mot. at 25. It would be absurd, as Bright Data emphasizes in its hypothetical, that someone who opens a Facebook account for seconds, or even minutes, before deleting that account would be “permanently giving up important legal rights the rest of society enjoys, and that they too enjoyed just minutes before, with no opportunity to ever get them back.” *Id.* While visitors to Facebook would not be contractually barred from automated scraping of public information, a user who briefly signs up with Facebook for entirely legitimate reasons would be barred for life from that same conduct.<sup>7</sup> *Cf. hiQ II*, 639 F. Supp. 3d at 964 (“hiQ would have the Court construe

---

<sup>7</sup> Some of the cases Bright Data cites for the proposition that courts reject perpetual interpretations of survival clauses, *see* Mot. at 25, are distinguishable from the present case. In two of these cases, *Webb Candy, Inc. v. Walmart Stores Inc.*, No. 09-CV-2056, 2010 WL 2301461, at \*6 (D. Minn. June 7, 2010), and *Ta Chen Int’l, Inc. v. Benada Aluminum Prods., LLC*, No. 20-cv-659, 2021 WL 7541515, at \*7 (M.D. Fla. May 13, 2021), courts construed the applicable survival clauses narrowly to avoid rendering expiration clauses obsolete. In another case, *Comcast Corp. v. Rovi Corp.*, No. 16-CV-3852, 2016 WL 7235802, at \*4 (S.D.N.Y. Dec. 16, 2016), the court limited a perpetual survival clause because the patent at issue had expired and conduct cannot “arise from” an expired patent. Other cases, *see, e.g., Uniloc 2017 LLC v. Google LLC*, 52 F.4th

1 LinkedIn’s User Agreement as prohibiting anyone from ever using its own service. No reasonable  
2 user would so interpret the User Agreement. hiQ thus fails to offer any evidence supporting  
3 substantive unfairness of the User Agreement.”).

4 In support of its interpretation of the survival clause as barring logged-out scraping in  
5 perpetuity, Meta argues that any other interpretation would make the clause superfluous. If “use”  
6 of Facebook applied only to logged-in activity, there would be no need for a survival clause as a  
7 user’s obligations would not survive account termination. Meta’s Sur-Reply at 6-7. Furthermore,  
8 the survival clause must be interpreted to impose continuing contractual obligations after users  
9 delete their accounts, rather than “to sue users that deleted their accounts for violations committed  
10 *before* they deleted their accounts” (as Bright Data argues). *Id.* at 7. Any other interpretation,  
11 Meta says, would “nullify the survival clause because it interprets the clause as establishing  
12 nothing but the same contractual obligations—and the same ability for Meta to enforce those  
13 obligations—that the Terms establish *without* the survival clause.” *Id.* (emphasis in original).  
14 Meta argues that, to “give effect” to the survival clause and avoid rendering it “superfluous,” the  
15 clause “must establish something more than the right to sue for pre-account deletion breaches.”  
16 *Id.*

17 However, Meta’s argument is not persuasive. First, the survival clause has utility in  
18 assuring the ability to enforce pre-termination breaches. It insures that, for instance, Meta’s  
19 choice of law and venue continues to apply. Moreover, Bright Data concedes that the clause  
20 permits enforcement of Meta’s rights even for post-termination conduct if they are based on pre-  
21 termination breaches (*e.g.*, post-termination sale of data obtained pre-termination). Further, as  
22 noted above, there are other provisions apart from enforcement rights (such as protection of  
23 Meta’s intellectual property rights) that are preserved by the survival clause. Thus, even as  
24 construed by Bright Data, the survival clause of section 4.2 is not superfluous.

25  
26 \_\_\_\_\_  
27 1352, 1358 (Fed. Cir. 2022), discuss rights that courts have determined “by their nature” survive  
28 termination, such as forum selection clauses. Nevertheless, the principle that survival clauses are  
generally limited to “conduct that arises out of or shares a nexus to,” the agreement at issue still  
stands and is applicable to the present case. *Nolde Bros.*, 430 U.S. at 249; Bright Data’s Mot. at  
25.

Based on the rules of contract construction that require consideration of the text and related structure of the contract, resolution of ambiguities against the drafter, and the disfavoring of provisions which appear to extend in perpetuity particularly as it affects access to public information on the Internet, the Court concludes that the survival clause does not prohibit logged-off, post-termination scraping unrelated to pre-termination breaches.<sup>8</sup>

ii. The Instagram Terms do not prohibit post-termination scraping

The Instagram Terms do not prohibit post-termination scraping because those Terms do not have a survival clause. The survival clause from the Meta Terms do not apply. The Instagram Terms expressly state that the Meta Terms of Service (which apply to Facebook and other products) do not apply to the use of Instagram. Munkittrick Decl. Ex 2 (“The Meta Terms of Service do not apply to [Instagram].”).

Meta attempts to read an implicit survival provision into the Instagram Terms, arguing that the Terms prohibit “ever” selling data from Instagram while a user had an active Instagram account, even if the user has since deleted that account. Meta’s Opp. at 12. But the word “ever” does not appear in the Instagram provisions prohibiting the sale of data. The Instagram Terms simply say that “[y]ou can’t sell, license, or purchase any account or data obtained from us or our Service.” Munkittrick Decl. Ex. 2. Nothing provides that this provision survives termination.

As the ban on scraping does not apply under Facebook’s Terms which contains a survival

---

<sup>8</sup> Because the Court interprets the Terms as not applicable to bar the post-termination scraping of public data by one no longer a user of Meta, the Court does not address Bright Data’s claim of unconscionability. It notes, however, the application of the Restatement (Second) of Contracts to the survival clause as construed by Meta would raise serious questions. The Restatement provides a two-part test to determine the reasonableness of a restraint on trade. First, the Court determines whether the restraint on trade is “ancillary” (or “contribut[ing] to” and “relat[ed]”) to an otherwise valid contractual relationship or transaction. Rest. 2d of Contracts § 187; *Blackburn v. Sweeney*, 53 F.3d 825, 829 (7th Cir. 1995). If the restraint is *not* ancillary to the relationship or transaction, it is *per se* illegal. Rest. 2d of Contracts § 187. “A restraint that is not so related to an otherwise valid transaction or relationship is necessarily unreasonable.” Rest. 2d of Contracts § 187 cmt. b (emphasis in original); *accord Blackburn*, 53 F.3d at 828 (finding a “covenant not to compete” of “infinite duration” with “no time limit” was “naked, not ancillary, and *per se* illegal to boot”).

Second, even if the restraint is ancillary, it must be narrowly tailored in time and scope to a legitimate interest to be enforceable. Rest. 2d of Contracts § 188. Such an ancillary restraint is unenforceable if (a) the restraint is greater than is needed to protect the promisee’s legitimate interest, or (b) the promisee’s need is outweighed by the hardship to the promisor and the likely injury to the public. Rest. 2d § 188(1).

clause, for the reasons stated above, it follows *a fortiori* that any ban by Instagram’s Terms would not apply to post-termination scraping.

B. Breach and Damages

Having found no evidence that Bright Data engaged in logged-in scraping and that Bright Data’s logged-out scraping of public data does not violate Meta’s of Instagram Terms, there is no basis to find a breach of contract by Bright Data and hence no basis for damages. As for any alleged continuing breach, because the Court found the Terms do not prohibit post-termination logged-out scraping of public data, no claim for any such breach lies.

Accordingly, Meta’s motion for partial summary judgment on the issue of liability for breach of contract is **DENIED**.

**IV. BRIGHT DATA’S MOTION FOR SUMMARY JUDGMENT**

When considering cross-motions for summary judgment, the Court must consider “[e]ach motion . . . on its own merits.” *Celotex*, 477 U.S. at 322. Bright Data seeks summary judgment in its favor that: (1) there was no contract formed between Bright Data and Meta due to lack of (i) mutual assent and (ii) consideration; (2) that the Meta Terms do not prohibit using public data from Meta after user accounts are terminated, and (3) that Meta cannot succeed on quasi-contractual claims.

A. Bright Data did not breach the Terms by its logged-out scraping of public data

Bright Data concedes that it was bound to Meta’s Terms while it had Facebook and Instagram accounts, *see* Holtzblatt Decl. Ex. D at 8, and that it sells data collected from Facebook and Instagram. Kol Decl. at ¶¶ 29-30; Karumudi Decl. Ex. A. However, even viewing the evidence in the light most favorable to the non-moving party (Meta), for the reasons stated above in the context of Meta’s motion, the Facebook and Instagram Terms do not bar logged-off scraping of public data; perforce it does not prohibit the sale of such public data. Therefore, the Terms cannot bar Bright Data’s logged-off scraping activities. This is especially true, as noted above, with respect to post-termination scraping of public data as no survival clause applies.

As noted above, interpretation of the Terms is a question for the court as a matter of law. Because Meta has provided no evidence of logged-in scraping, there is no genuine dispute of

material fact on this issue. Accordingly, the undisputed evidence establishes that Bright Data only engaged in logged-out scraping of public data unrelated to its accounts with Meta and thus did not breach the Terms either while it had accounts with Facebook and Instagram or after terminating its accounts.

Accordingly, the Court **GRANTS** Bright Data's motion for summary judgment on the issue of breach of contract.

B. The complaint does not state an independent quasi-contract claim for unjust enrichment

Meta contends that it is entitled to restitution because Bright Data has been unjustly enriched through its sale of Facebook and Instagram data obtained through unauthorized automated means. Meta's Opp. at 29. According to Meta, it

provides a benefit in the form of its Facebook and Instagram services. . . . And Bright Data concedes that it generates revenue by selling user data and helping others use unauthorized automated means to circumvent Meta's access restrictions to access and collect data from those services. . . . Bright Data's ability to profit from such conduct is inherently unjust.

Meta's Opp. at 29 (citing Kol Decl. ¶¶ 34-36).

As the complaint currently stands, however, Meta has simply asserted an unjust enrichment theory as part of its claim for breach of contract. Compl. ¶ 71. Meta has not pled an independent quasi-contract claim for unjust enrichment. *See Astiana v. Hain Celestial Grp., Inc.*, 783 F.3d 753, 762 (9th Cir. 2015) ("In California, there is not a standalone cause of action for 'unjust enrichment,' which is synonymous with 'restitution.'"). Because the Court has dismissed the claim for breach of contract, and Meta has not pled an alternative claim for quasi-contract, the Court does not address whether an alternative claim for unjust enrichment independent of contract can be stated. The Court is also reluctant to address any quasi-contract claim given that the parties' briefs did not fully address such a claim independent of the asserted contract claim. If Meta wishes to amend its complaint to assert such a claim, it may do so.

V. CONCLUSION

For the aforementioned reasons, the Court **DENIES** Meta's motion for partial summary judgment on the issue of liability for breach of contract. The Court also **GRANTS** Bright Data's

1 motion for summary judgment in its favor on the issues of breach of contract. If Meta wishes to  
2 amend its complaint to add a claim for quasi-contract, it may do so. Such a complaint must be  
3 filed within three weeks of the date of this order.

4 Based on the rulings above, the only claim remaining against Bright Data is the claim for  
5 tortious interference with contract. The Court hereby sets a status conference for March 5, 2024,  
6 at 2:30 p.m., so that it may discuss with the parties the litigation of this remaining claim. The  
7 parties shall file a joint status report one week in advance of the conference.

8 This order disposes of Docket Nos. 75 and 105.

9  
10 **IT IS SO ORDERED.**

11  
12 Dated: January 23, 2024

13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

  
EDWARD M. CHEN  
United States District Judge