

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

X CORP.,

Plaintiff,

v.

BRIGHT DATA LTD.,

Defendant.

No. C 23-03698 WHA

ORDER DISMISSING COMPLAINT

INTRODUCTION

A social media company asserts breach-of-contract and tort claims against a data-scraping company. It seeks to bar the data-scraping company from extracting and copying public data from its social media platform, and from selling tools that enable others to extract and copy public data from its social media platform. Meanwhile, the social media company sells its own tools that enable others to extract and copy public data from its social media platform.

The data-scraping company has moved to dismiss for lack of personal jurisdiction and failure to state a claim. A prior order denied the motion to dismiss as to lack of personal jurisdiction. For the reasons stated herein, the motion to dismiss as to failure to state a claim is **GRANTED** and the instant complaint is **DISMISSED**.

Our court of appeals has held that giving social media companies “free rein to decide, on any basis, who can collect and use data — data that the companies do not own, that they otherwise make publicly available to viewers, and that the companies themselves collect and use — risks the possible creation of information monopolies that would disserve the public interest.” *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1202 (9th Cir. 2022). With that in mind, this district court carefully considered each of the claims asserted. It now concludes that none of the claims passes muster.

STATEMENT

Plaintiff X Corp. owns and operates the social media platform X, formerly known as Twitter (Amd. Compl. ¶¶ 1, 17). X has hundreds of millions of active users worldwide, with more than twenty-three million accounts registered from California (Amd. Compl. ¶ 18).¹

Those who register for accounts on X can post comments, images, and videos, as well as interact with others who have registered for accounts on X by re-posting, liking, and commenting on their posts (Amd. Compl. ¶¶ 19–20). Those who do not register for accounts on X can still access the platform, however (Amd. Compl. ¶¶ 22, 37). According to X Corp., “[a]ll users who register for a X account, and/or view the X website or application agree to a binding contract with X Corp. as outlined in X Corp.’s User Agreement, which is comprised of the Terms of Service, Privacy Policy, and the Rules and Policies (collectively the ‘Terms’)” (Amd. Compl. ¶ 22).

1. PERTINENT PROVISIONS.

The Terms inform an X user of “Your Rights and Grant of Rights in the Content.” Specifically, they provide that “[y]ou retain your rights to any Content you submit, post or display on or through the Services.” In other words, “[w]hat’s yours is yours — you own your Content” (Terms 4). “Services” are broadly defined as “our various websites, SMS, APIs, email notifications, applications, buttons, widgets, ads, commerce services, and our other covered services . . . that link to these Terms” (Terms 2–3). “Content” is broadly defined as

¹ For readability, internal quotation marks and citations within citations are omitted throughout unless otherwise noted.

1 “any information, text, links, graphics, photos, audio, videos, or other materials or
2 arrangements of materials uploaded, downloaded or appearing on the Services” (Terms 3).²

3 The Terms further provide that “[b]y submitting, posting or displaying Content on or
4 through the Services, you grant us a worldwide, non-exclusive, royalty-free license (with the
5 right to sublicense) to use, copy, reproduce, process, adapt, modify, publish, transmit, display
6 and distribute such Content in any and all media or distribution methods now known or later
7 developed” (Terms 4–5). This non-exclusive “license authorizes us to make your Content
8 available to the rest of the world and to let others do the same” (Terms 5; *see also* Terms 1).

9 Meanwhile, the Terms restrict many forms of “Misuse of the Services” (Terms 8). These
10 restrictions are the fulcrum of the instant complaint. Relevant here, the Terms provide that
11 “[i]f you want to reproduce, modify, create derivative works, distribute, sell, transfer, publicly
12 display, publicly perform, transmit, or otherwise use the Services or Content on the Services,
13 you must use the interfaces and instructions we provide, except as permitted through the
14 Services, these Terms, or the [developer] terms Otherwise, all such actions are strictly
15 prohibited” (Terms 6; *see* Amd. Compl. ¶ 29). Separately, the Terms ban an X user from
16 scraping, unambiguously stating that “scraping the Services in any form, for any purpose
17 without our prior written consent is expressly prohibited” (Terms 8; *see* Amd. Compl. ¶ 25).

18 As our court of appeals has explained, “[s]craping involves extracting data from a
19 website and copying it into a structured format, allowing for data manipulation or analysis,”
20 usually by automated means, *i.e.*, a computer script that requests and retrieves information.
21 *hiQ Labs*, 31 F.4th at 1186 n.4. Unlike a browser, which requests and retrieves information for
22 display to an internet user, a scraper requests and retrieves information for another purpose,
23 often a more tailored one, *e.g.*, to extract and copy the court dates of inmates published daily

24
25 ² In evaluating a motion to dismiss, “a court may consider a writing referenced in a complaint but
26 not explicitly incorporated therein if the complaint relies on the document and its authenticity is
27 unquestioned.” *Swartz v. KPMG LLP*, 476 F.3d 756, 763 (9th Cir. 2007). This order considers
28 the Terms referenced in plaintiff’s instant complaint, using the pagination of Exhibit 1 to
defendant’s motion to dismiss where applicable for convenience (*see* Dkt. No. 42-1, Munkittrick
Decl. Exh. 1). “Terms 3” corresponds to the third page of X Corp.’s Terms of Service, dated
September 29, 2023, and available on X Corp.’s website at the time of writing. X Corp. Terms of
Service, <https://twitter.com/en/tos> (last visited May 9, 2024) [<https://perma.cc/NPM5-FHYP>].

1 by a county jail to help journalists better understand the inmates’ trajectories through the
2 system.³

3 It bears emphasis that this action deals only with scraping data that X Corp. has made
4 publicly available. X Corp. does not allege or in any way suggest that the data scraped was
5 solely accessible to X users logged in to registered accounts or was otherwise password-
6 protected. Rather, it points to materials advertising “techniques to scrape, structure, and
7 analyze public web data” and “[t]ap into . . . public accounts,” as well as tools used to “gather
8 vast amounts of public web data” (Amd. Compl. ¶¶ 45, 50, 64). X Corp. “employs rate limits
9 that cap the number of posts that may be viewed by registered users and those who access the
10 platform without an account,” but that does not render public posts any less public (Amd.
11 Compl. ¶ 37). Nor do the other “industry standard automation prevention techniques” that
12 X Corp. implements, such as CAPTCHAs and anomaly detection tools (Amd. Compl. ¶ 35).

13 In addition to the ban on scraping, the Terms provide for other technical restrictions.
14 For example, an X user may not “access, tamper with, or use non-public areas of the Services,
15 our computer systems, or the technical delivery systems of our providers” (Terms 8; *see* Amd.
16 Compl. ¶ 23). An X user also may not “access or search or attempt to access or search the
17 Services by any means (automated or otherwise) other than through our currently available,
18 published interfaces that are provided by us (and only pursuant to the applicable terms and
19 conditions), unless you have been specifically allowed to do so in a separate agreement with
20 us” (Terms 8; *see* Amd. Compl. ¶ 24).

21 Moreover, the Terms restrict an X user from selling data from X. Again, “Content” is
22 broadly defined as “any information, text, links, graphics, photos, audio, videos, or other
23 materials or arrangements of materials uploaded, downloaded or appearing on the Services”
24 (Terms 3). And, an X user may not “sell . . . the Services or Content on the Services” unless
25 otherwise authorized (Terms 6; *see* Amd. Compl. ¶ 29). But, “[f]or developers who wish to
26

27 ³ David Eads, *How (and Why) We’re Collecting Cook County Jail Data*, PROPUBLICA (July 24,
28 2017), <https://www.propublica.org/nerds/how-and-why-collecting-cook-county-jail-data>
[<https://perma.cc/YW4Y-VWCJ>].

1 retrieve or analyze X Corp.’s data, X Corp. offers specialized access to its Application
2 Programming Interfaces (‘APIs’) through a tiered subscription service,” *i.e.*, for a fee (Amd.
3 Compl. ¶ 32). So, X Corp. allows for the sale of data extracted and copied from X but only if
4 X Corp. is paid for it. X Corp. otherwise restricts the sale of data extracted and copied from X
5 by prohibiting an X user from scraping and selling data from the platform.

6 **2. PRESENT ALLEGATIONS.**

7 Defendant Bright Data Ltd. is a data-scraping company (Amd. Compl. ¶ 6). According
8 to Bright Data, “[i]ts suite of technologies and services help Fortune 500 companies, academic
9 institutions, and small businesses retrieve and synthesize vast amounts of public information”
10 (Br. 3). There are three types of products that Bright Data offers: (1) datasets built from data
11 that Bright Data scrapes itself, (2) scraping tools that enable their purchasers to scrape data
12 themselves, and (3) proxy network services that enable their purchasers to scrape data through
13 proxy servers, using those servers’ IP addresses (Amd. Compl. ¶¶ 50–51, 55–58, 63–64; Br. 4).

14 In this lawsuit, X Corp. alleges that Bright Data scrapes data from X and sells data
15 scraped from X, using elaborate technical measures to evade X Corp.’s anti-scraping
16 technology, while facilitating its customers in and inducing them to scrape data from X —
17 all in violation of the Terms to which Bright Data and its customers are bound (Amd. Compl.
18 ¶¶ 1–2). How so? X Corp. contends that Bright Data and its customers are bound as X users.
19 Specifically, X Corp. contends that Bright Data is bound (1) by a “browser-wrap” or “browse-
20 wrap” contract, having used X Corp. services in the act of scraping data from X, impliedly
21 agreeing to the Terms in the process; and (2) by a “click-wrap” or “click-through” contract,
22 having registered an account (@bright_data) to promote Bright Data products, expressly
23 agreeing to the Terms as early as February 2016 (Amd. Compl. ¶¶ 39–41; *see also* Amd.
24 Compl. ¶ 44). Meanwhile, Bright Data customers are conceivably likewise bound by browser-
25 wrap and click-wrap contracts, having used X Corp. services in the act of scraping data from
26 X and, in some instances, having registered accounts (*see* Amd. Compl. ¶¶ 22, 55, 63).

27 X Corp. does not allege that Bright Data has used its own account, or any other account,
28 to scrape data from X. Nor does X Corp. allege that Bright Data customers have used their

own accounts, or any other accounts, to do so. All X Corp. alleges is that Bright Data and its customers have scraped data from X, violating the Terms to which they were bound due to their use of the services in scraping (forming browser-wrap contracts) and, in some cases, account registration prior to scraping (forming click-wrap contracts). These contracts will be discussed in greater detail below.

3. PROCEDURAL HISTORY.

In a first complaint filed in July 2023, X Corp. sued Bright Data, asserting claims for breach of contract, tortious interference with contract, and unjust enrichment (Dkt. No. 1). Bright Data then filed a first motion to dismiss in October 2023 (Dkt. No. 22). It moved to dismiss the tortious-interference claim for lack of personal jurisdiction under Rule 12(b)(2) and broadly moved to dismiss for failure to state a claim under Rule 12(b)(6).

In November 2023, X Corp. filed an amended complaint, asserting additional claims for trespass to chattels, violation of California Business and Professions Code Section 17200, and misappropriation (Dkt. No. 36). An order denied Bright Data's original motion to dismiss as moot, and another order allowed the parties extra pages for briefing a subsequent motion to dismiss (Dkt. Nos. 37, 41).

In December 2023, Bright Data filed the pending motion to dismiss, along with a motion to stay discovery (Dkt. Nos. 42–43). It has moved to dismiss the tort claims for lack of personal jurisdiction under Rule 12(b)(2) and, again, broadly moved to dismiss for failure to state a claim under Rule 12(b)(6).

At the hearing, the judge denied the motion to stay discovery and took the motion to dismiss under submission, requesting supplemental briefing on issues raised in that motion (Dkt. Nos. 55, 59; *see* Dkt. Nos. 60–61, 63–64). And, with its supplemental briefing, Bright Data concurrently filed a motion for summary judgment on the breach-of-contract claim, which was then fully briefed (Dkt. Nos. 62, 69–70). Because the judge finds the breach-of-contract claim suitable for dismissal with the tort claims, the later-filed motion for summary judgment is **DENIED AS MOOT**, but this order takes arguments raised in the briefing of that motion into account.

After the hearing, an order denied the motion to dismiss under Rule 12(b)(2), having found that Bright Data had sufficient contacts with California and the district (Dkt. No. 67). This order considers Bright Data's motion to dismiss under Rule 12(b)(6), granting the motion and dismissing all claims. It follows full briefing and oral argument.

ANALYSIS

A complaint must plead "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). A claim to relief is plausible "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). Although the district court must accept well-pleaded factual allegations as true, "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Id.* at 678–79. Dismissal under Rule 12(b)(6) "can be based on the lack of a cognizable legal theory or the absence of sufficient facts alleged under a cognizable legal theory." *Balistreri v. Pacifica Police Dep't*, 901 F.2d 696, 699 (9th Cir. 1988).

Fundamentally, X Corp. has two grievances that it seeks to redress by way of the instant complaint. *First*, according to X Corp., Bright Data has *improperly accessed its systems* and assisted others in improperly accessing its systems (*e.g.*, servers, routers, networks). *Second*, according to X Corp., Bright Data has *improperly scraped and sold its data*, and assisted others in improperly scraping its data (*e.g.*, comments, images, likes). Put another way, X Corp. seeks to vindicate an interest both in *systems accessed* and in *data scraped and sold*.

This order takes up the two grievances separately, recognizing that some of X Corp.'s claims turn on one, some turn on the other, and some turn on both. With its claims for trespass to chattels and fraudulent violation of Section 17200, X Corp. seeks to establish liability for access to systems. With its claims for misappropriation and unjust enrichment, X Corp. seeks to establish liability for scraping and selling of data. And, with its claims for tortious interference with contract and breach of contract, X Corp. seeks to establish liability for both access to systems and scraping and selling of data. "[A] breach of contract is often framed as one claim for relief, with multiple theories supporting said breach," and access, scraping, and

1 selling are all restricted by contract, X Corp.’s Terms. *Wehner v. Genentech, Inc.*, No. C 20-
2 06894 RS, 2022 WL 179683, at *3 (N.D. Cal. Jan. 20, 2022) (Judge Richard Seeborg).

3 The two-fold framing (accessing systems vs. scraping and selling data) will be used to
4 help explain why the instant complaint fails to state a claim upon which relief can be granted.
5 To the extent the claims are based on access to systems, they fail because X Corp. has alleged
6 no more than threadbare recitals of elements supported by conclusory statements. To the extent
7 the claims are based on scraping and selling of data, they fail because they are preempted by
8 federal law. Specifically, they fail because they stand as an obstacle to the accomplishment and
9 execution of the full purposes and objectives of Congress in enacting the Copyright Act.

10 **1. CLAIMS BASED ON ACCESS TO SYSTEMS.**

11 X Corp.’s interest in the systems accessed is clear cut. Surely, “the analogy between real
12 property and the internet is not perfect.” *Sandvig v. Barr*, 451 F. Supp. 3d 73, 88
13 (D.D.C. 2020) (Judge John D. Bates). But it is now well-established that some exchange of
14 information across privately owned servers, routers, and networks connected to the internet can
15 interfere with a personal property interest without depriving the owner of personal property in
16 the traditional sense. *See Van Buren v. United States*, 593 U.S. 374, 378 (2021).

17 Exchange of information across another’s internet-connected systems is to be expected.
18 The internet was designed to enable this exchange. Moreover, “a defining feature of public
19 websites is that their publicly available sections lack limitations on access” and “are open to
20 anyone with a web browser.” *hiQ Labs*, 31 F.4th at 1199. Whether some exchange of
21 information across a social media company’s internet-connected systems can support a claim
22 for relief is thus contextual. Here, X Corp.’s claims based on access to its internet-connected
23 systems are not plausibly pleaded.

24 **A. TRESPASS TO CHATTELS.**

25 We start with trespass to chattels, an old tort that is finding new life. According to
26 X Corp., Bright Data “intentionally entered into, and made use of, X Corp.’s technological
27 infrastructure . . . to obtain information for its own economic benefit” (Amd. Compl. ¶ 96).
28 Bright Data thereby “knowingly exceeded the permission granted by X Corp. to access its

personal property” and “caused other persons . . . to knowingly exceed the permission granted by X Corp. to access its personal property” (Amd. Compl. ¶¶ 97, 99). X Corp. contends that this “conduct constitutes trespass to X Corp.’s chattels” (Amd. Compl. ¶ 101).

The Supreme Court of California has held that “trespass to chattels lies where an intentional interference with the possession of personal property has proximately caused injury.” *Intel Corp. v. Hamidi*, 71 P.3d 296, 302 (Cal. 2003). As such, “an interference (not amounting to dispossession) is not actionable, under modern California and broader American law, without a showing of harm.” *Id.* at 303. “Short of dispossession, personal injury, or physical damage (not present here), intermeddling is actionable only if the chattel is impaired as to its condition, quality, or value, or . . . the possessor is deprived of the use of the chattel for a substantial time.” *Id.* at 306.

Critically, the instant complaint alleges no such impairment or deprivation. X Corp. parrots elements, reciting that Bright Data’s “acts have caused injury to X Corp. and . . . will cause damage in the form of impaired condition, quality, and value of its servers, technology infrastructure, services, and reputation” (Amd. Compl. ¶ 102). Its lone deviation from that parroting — a conclusory statement that Bright Data’s “acts have diminished the server capacity that X Corp. can devote to its legitimate users” — fails to move the needle (Amd. Compl. ¶ 98). To say nothing of the fact that, as alleged, Bright Data and its customers *are* legitimate X users (subject to the Terms), the scraping tools and services they use are reliant on X Corp.’s servers functioning exactly as intended. *See WhatsApp Inc. v. NSO Grp. Techs. Ltd.*, 472 F. Supp. 3d 649, 684 (N.D. Cal. 2020) (Judge Phyllis J. Hamilton).

Absent allegation, it cannot be assumed that Bright Data or its customers sending requests to X Corp.’s servers with a scraper is inherently burdensome, or inherently more burdensome than an X user sending requests to X Corp.’s servers with a browser. After all, “the load placed on the host’s server may in fact be *lighter*, because the scraper may only need one web resource, rather than the dozens a web-browser might need, in order to extract the relevant information.” Andrew Sellars, *Twenty Years of Web Scraping and the Computer*

1 *Fraud and Abuse Act*, 24 B.U. J. SCI. & TECH. 372, 387 (2018) (citing Ryan Mitchell, *Web*
2 *Scraping with Python* viii–ix (2015)).

3 Meanwhile, *Intel* rejected an attempt to bend trespass to chattels into a claim that could
4 remedy injury to reputation, warning of “br[eaking] the chain between the trespass and the
5 harm, allowing indirect harms to [a plaintiff’s] business interests . . . to count as harms to the
6 chattel (the server),” and “cut[ting] trespass to chattels free from its moorings of dispossession
7 or the equivalent, allowing the court free reign [*sic*] to hunt for ‘impairment.’” 71 P.3d at 307
8 (*sic* in original). *Intel* also held that time and money spent attempting to restrict access cannot
9 be “bootstrapped into an injury to [a plaintiff’s] possessory interest in its computers,” because
10 “[i]njury can only be established by the completed tort’s consequences, not by the cost of the
11 steps taken to avoid the injury and prevent the tort; otherwise, we can create injury for every
12 supposed tort.” *Id.* at 308. X Corp. should keep all of this in mind if it seeks leave to amend
13 the instant complaint. In any event, the facts now alleged are insufficient to state a claim for
14 trespass to chattels.

15 This order does not hold that sending requests to servers could never support a trespass-
16 to-chattels claim. By way of example, as our own Judge Edward Chen has observed, denial-
17 of-service attacks could prove remediable under this tort (inundating servers with requests,
18 often forcing them offline). *See hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099, 1113
19 n.11 (N.D. Cal. 2017). All that has been alleged here, however, is that Bright Data has sent
20 requests to X Corp. servers in violation of the Terms, which does not itself impair the servers
21 or deprive X Corp. of their use.

22 Nor does this order in any way suggest that X Corp. should refrain from implementing
23 technical measures to restrict access to its systems, *e.g.*, “CAPTCHAs, user identification and
24 IP rate limits and anomaly detection tools” (Amd. Compl. ¶ 35). Not only does the law decline
25 to forbid such measures, but it generally allows X Corp. to implement them. As observed in
26 *Intel*, “[s]ufficient legal protection of the possessor’s interest in the mere inviolability of his
27 chattel is afforded by his privilege to use reasonable force to protect his possession against
28

even harmless interference.” 71 P.3d at 303 (quoting Restatement (Second) of Torts § 218 cmt. e (Am. L. Inst. 1965)). But harmless interference cannot constitute trespass to chattels.

B. VIOLATION OF SECTION 17200.

We now turn to Section 17200 of the California Business and Professions Code. The provision prohibits unlawful, unfair, and fraudulent business acts. X Corp. alleges unlawful and fraudulent business acts (Amd. Compl. ¶¶ 103–06). Although X Corp. makes arguments in its opposition based on an unfair business act, that act was not alleged beyond bare recitation of the word “unfair” (*compare ibid.*, with Opp. 31–32). And, in the end, X Corp. will fail to show an unlawful business act because it will fail to state a predicate claim. *See, e.g., Eidmann v. Walgreen Co.*, 522 F. Supp. 3d 634, 647 (N.D. Cal. 2021) (Judge Edward J. Davila). This subsection therefore focuses on the alleged fraudulent business acts.

According to X Corp., Bright Data “deceived X Corp. into providing it access to, and information from, the X Corp. computer network” (Amd. Compl. ¶ 104). Specifically, X Corp. contends that (1) Bright Data’s “data-collection technology and data-scraping tools deliberately misrepresented the requests sent to the X platform, posing as legitimate X users,” and (2) Bright Data’s “sale of IP proxies masquerades as a legitimate X user to avoid X Corp.’s technical measures designed to prevent unauthorized access of its computer servers” (*ibid.*).

Fraud under Section 17200 “requires different elements than common law fraud” and “reflects the [law’s] focus on the defendant’s conduct, rather than the plaintiff’s damages.” *Pirozzi v. Apple, Inc.*, 966 F. Supp. 2d 909, 920 (N.D. Cal. 2013) (Judge Jon S. Tigar) (quoting *Boschma v. Home Loan Ctr., Inc.*, 129 Cal. Rptr. 3d 874, 893 (Cal. Ct. App. 2011)). Because the plaintiff’s economic injuries must arise as a result of fraudulent conduct, the plaintiff must allege a causal connection or reliance on a misrepresentation, pointing to a misrepresentation with particularity and pleading that it was an immediate cause of injury-producing conduct. *Ibid.* Yet, as alleged here, any misrepresentation remains elusive — all the more so considering the heightened pleading standard to which fraud claims are subject. Fed. R. Civ. P. 9(b); *see Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1125 (9th Cir. 2009).

1 Starting with the argument that Bright Data’s technology and tools misrepresented
2 requests, remember X Corp. does not allege that Bright Data or its customers have used their
3 own registered accounts, or any other registered accounts, to scrape data from X, *i.e.*, to access
4 X by sending requests to X Corp.’s servers (for extracting and copying data). Meanwhile,
5 X Corp. acknowledges that one does not need a registered account to access X and send such
6 requests (*see* Amd. Compl. ¶ 22). X Corp. also acknowledges that X users with registered
7 accounts can access X and send such requests *without logging in* to their registered accounts
8 (and that they are still bound by the Terms in this case) (*see* Amd. Compl. ¶¶ 20, 22).

9 That is all Bright Data and its customers have done insofar as the instant complaint
10 reveals. They did not misrepresent themselves, “posing as legitimate X users,” but rather acted
11 as legitimate X users who were under no obligation to log in. It is unclear how Bright Data or
12 its customers could be construed as *misrepresenting* requests sent under these circumstances.
13 That “how” is necessary at the pleading stage. *See Doe v. SuccessfulMatch.com*, 70 F. Supp.
14 3d 1066, 1081–82 (N.D. Cal. 2014) (Judge Lucy H. Koh).

15 As for Bright Data’s sale of IP proxies, X Corp. appears to insinuate that the use of
16 different IP addresses is inherently deceptive. But an internet user is not assigned a unique IP
17 address. Rather, as our court of appeals has explained, “[e]very computer or server connected
18 to the Internet has a unique IP address.” *United States v. Forrester*, 512 F.3d 500, 510 n.5 (9th
19 Cir. 2008). Accordingly, internet users can have different IP addresses simply by virtue of
20 using different devices (*e.g.*, smartphone, laptop, desktop) across different connections
21 (*e.g.*, cellular network, home network, work network). Internet users can also change the IP
22 addresses they use to request and retrieve information (*e.g.*, using virtual private networks).
23 *See United States v. Kvashuk*, 29 F.4th 1077, 1084 n.4 (9th Cir. 2022). What’s more, “IP
24 addresses can be dynamic,” with “the number chang[ing] each time the computer accesses the
25 Internet.” *United States v. Norris*, 942 F.3d 902, 904 n.2 (9th Cir. 2019). None of this is
26 inherently deceptive.

27 Bright Data offers proxy network services. “A proxy server ‘hides’ a computer’s IP
28 address[,] serving as an intermediary computer — a ‘middle man’ — between the website and

the [internet] user,” allowing internet users to request and retrieve information using intermediary computers with those computers’ IP addresses. *Tagged, Inc. v. Does 1 through 10*, No. C 09-01713 WHA, 2010 WL 370331, at *2 n.1 (N.D. Cal. Jan. 25, 2010). As Bright Data recognizes, at most, X Corp. seems to allege that its proxy servers deceptively omit identifying information in the process (Br. 32). There is no affirmative duty that requires an internet user to identify oneself with a given IP address when connecting to the internet, however. “[A] failure to disclose a fact one has no affirmative duty to disclose is [not] ‘likely to deceive’ anyone” within the meaning of Section 17200. *Hodsdon v. Mars, Inc.*, 891 F.3d 857, 868 (9th Cir. 2018) (quoting *Daugherty v. Am. Honda Motor Co.*, 51 Cal. Rptr. 3d 118, 128 (Cal. Ct. App. 2006)) (alteration in original). That Bright Data sells IP proxies does not itself state a claim for fraudulent violation of Section 17200.

Again, this order does not hold that sending requests to servers could never support a fraudulent violation of Section 17200 claim. Consider the following situation. A corporate user of a social media platform logs in to a registered account on that platform and sends requests to the social media company’s servers in carrying out a harmful activity. The social media company terminates the corporate user’s account with an explanation and admonition to never come back. The corporate user then comes back using a different account and sends requests to the social media company’s servers in carrying out the same harmful activity. In that case, the corporate user’s misrepresentation would be the immediate cause of injury-producing conduct. No such facts are alleged here.

And, once more, this order does not in any way suggest that X Corp. should refrain from engaging in “technological self-help” to restrict access to its systems. *hiQ Labs*, 273 F. Supp. 3d at 1113 n.11. The law allows X Corp. to undertake reasonable measures to protect its possession. But the use and sale of scraping tools and services is not inherently fraudulent barring allegations that a misrepresentation has, in fact, occurred.

C. TORTIOUS INTERFERENCE WITH CONTRACT.

Next, we turn to tortious interference. According to X Corp., “[b]y offering services and tools designed to provide automated access to the X platform, and to scrape data from the

platform, [Bright Data] induced a breach or disruption of the Terms by X users” (Amd. Compl. ¶ 83) (emphasis added). To the extent the theory of breach or disruption is automated access, it will be discussed now. To the extent the theory of breach or disruption is scraping data, it will be discussed in the subsequent section.

The elements of a tortious interference with contractual relations claim are (1) a valid contract between plaintiff and a third party, (2) defendant’s knowledge of this contract, (3) defendant’s intentional acts designed to induce breach or disruption of the contractual relationship, (4) actual breach or disruption of the contractual relationship, and (5) resulting damage. *Pac. Gas & Elec. Co. v. Bear Stearns & Co.*, 791 P.2d 587, 589–90 (Cal. 1990).

At the outset, this order rejects Bright Data’s argument that X Corp. has failed to allege the existence of valid, enforceable third-party contracts such that X Corp. cannot state a claim based on the breach or disruption of those contracts. X Corp. alleges that Bright Data has sold a “Scraping Browser” that Bright Data has specifically marketed for scraping data from X (Amd. Compl. ¶ 60 (citing Exh. G)). X Corp. further alleges that Bright Data has sold tools specifically designed to scrape data from X (Amd. Compl. ¶ 58 (citing Exhs. F–I)). Bright Data does not contest these allegations. Nor does it offer any reason to believe that it has never sold these tools, or that they have never been used to scrape data from X, or that no Bright Data customers have ever been X users bound by the Terms.

Read in the light most favorable to the non-movant, there are at least some Bright Data customers that have purchased the tools specifically designed to scrape data from X and used them to scrape data from X while being bound by the Terms, *e.g.*, those with registered accounts seeking to improve their footprint on the platform. Accordingly, read in the light most favorable to the non-movant, there are at least some X users that Bright Data has induced to breach. X Corp. does not identify those X users in the instant complaint, but X Corp. would not have had access to Bright Data customer information when drafting it. As Bright Data acknowledged at the hearing, it has taken pains “to protect [its] customers’ identities,” producing “customer specific information” while “anonymiz[ing] the identifying information” in another action (Tr. 51:5–12; *see also* Opp. 21).

1 X Corp. is not yet out of the woods, however. Although it has plausibly pleaded breach
2 (and disruption) of contractual relationships, it has not plausibly pleaded Bright Data’s tortious
3 interference under this theory of breach. Here, an exchange from the hearing is illustrative.
4 When the judge asked, “so you can’t even tell me if they are intruding?” counsel for X Corp.
5 responded, “we can’t,” noting that “we don’t know exactly how much intrusion there has been”
6 and that all X Corp. does know is that Bright Data “sell[s] data that [it] could have only gotten”
7 that way (Tr. 10:21–11:7). Therein lies the rub.

8 Among the elements of a tortious-interference claim is *resulting damage*. *Pac. Gas*
9 *& Elec.*, 791 P.2d at 590. The only damage that X Corp. plausibly pleaded in the instant
10 complaint is that resulting from scraping and selling of data and, by extension, inducing
11 scraping. X Corp. has not alleged *any damage* resulting from automated access to systems
12 and, by extension, inducing automated access. As explained above, X Corp. has pleaded no
13 impairment or deprivation of X Corp. servers resulting from sending requests to those servers.
14 And, thin allusions to server capacity that could be devoted to “legitimate users” and
15 reputational harm — not redressable under trespass to chattels as a matter of law — are simply
16 too conclusory to be redressable at all. X Corp. will be allowed to seek leave to amend to
17 allege damage (if any) resulting from automated access, as set out at the end of this order. But
18 the instant complaint has failed to state a claim for tortious interference based on such access.

19 **D. BREACH OF CONTRACT.**

20 Finally, we turn to breach of contract. X Corp. alleges that Bright Data “has breached,
21 and continues to breach, X Corp.’s Terms by *accessing the platform through unauthorized*
22 *means* and scraping data from the platform,” as well as “selling data that [Bright Data] has
23 scraped from X Corp.’s platform” (Amd. Compl. ¶¶ 73, 75) (emphasis added). To the extent
24 the theory of breach is access through unauthorized means, it will be discussed now. To the
25 extent the theory of breach is scraping and selling of data, it will be discussed in the subsequent
26 section.

27 The elements of a breach-of-contract claim are (1) the existence of a contract,
28 (2) plaintiff’s performance or excuse for nonperformance, (3) defendant’s breach, and

(4) resulting damage. *Oasis W. Realty, LLC v. Goldman*, 250 P.3d 1115, 1121 (Cal. 2011). Here too, we begin with the viability of the alleged breach. This order rejects Bright Data’s argument that X Corp. has failed to allege an existing enforceable contract with Bright Data such that X Corp. cannot state a breach-of-contract claim based on the breach of that contract.

Consider the “two flavors” of contracts discussed previously: click-wrap contracts that hinge on express assent, and browser-wrap contracts that hinge on implied assent. *See Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1176 (9th Cir. 2014). Bright Data acknowledges that it registered the @bright_data account, agreeing to X Corp.’s Terms by way of a click-wrap contract as early as February 2016 (Br. 1; *see also* Amd. Compl. ¶ 41). Meanwhile, Bright Data acknowledges that it scrapes data from X, which X Corp. alleges binds Bright Data by way of a browser-wrap contract (Br. 3; Amd. Compl. ¶ 40). According to Bright Data, however, there is no longer an enforceable contract because it shut down the @bright_data account (among others), thereby terminating its click-wrap contract, and it has not impliedly agreed to the Terms in ongoing scraping, thereby forming a browser-wrap contract (Br. 1; Dkt. No. 62 at 1). Even assuming that Bright Data did shut down its registered account(s) and that this had the effect of terminating its click-wrap contract(s) with X Corp. — which was disputed across many briefs — that is of no consequence.

As our court of appeals has explained, “[u]nless the website operator can show that a consumer has actual knowledge of the agreement, an enforceable [browser-wrap] contract will be found based on an inquiry notice theory only if (1) the website provides reasonably conspicuous notice of the terms to which the consumer will be bound; and (2) the consumer takes some action, such as clicking a button or checking a box, that unambiguously manifests his or her assent to those terms.” *Berman v. Freedom Fin. Network, LLC*, 30 F.4th 849, 856 (9th Cir. 2022) (emphasis added). Make no mistake, *Berman* (and the California law on which it rests) should insulate many from entering into enforceable contracts with X Corp. *See id.* at 864–68 (Judge M. Miller Baker, concurring). But it cannot insulate Bright Data, a party with actual knowledge of the Terms at all relevant times (and a sophisticated party to boot).

1 Even assuming that Bright Data shut down its registered account(s) and that this had the
2 effect of terminating its click-wrap contract(s) with X Corp., there is no question that Bright
3 Data remained bound by the Terms, having impliedly agreed to them in ongoing scraping.
4 Bright Data had actual knowledge of the Terms and the fact that the Terms restricted, *inter*
5 *alia*, “access[ing] . . . or attempt[ing] to access . . . the Services by any means (automated or
6 otherwise),” “scraping the Services in any form, for any purpose,” and “sell[ing] . . . Content
7 on the Services” as Bright Data proceeded to do just that (Terms 6, 8). And, “courts have
8 consistently enforced browsewrap agreements where the user had actual notice of the
9 agreement.” *Nguyen*, 763 F.3d at 1176.

10 Once more, however, X Corp. is still in the woods. Among the elements of a breach-of-
11 contract claim is *resulting damage*. *Oasis*, 250 P.3d at 1121. Under California law, “[a]
12 breach of contract without damage is not actionable.” *Aguilera v. Pirelli Armstrong Tire*
13 *Corp.*, 223 F.3d 1010, 1015 (9th Cir. 2000) (quoting *Pat. Scaffolding Co. v. William Simpson*
14 *Const. Co.*, 64 Cal. Rptr. 187, 191 (Cal. Ct. App. 1967)). Although nominal damages may be
15 available in the absence of actual damages, “[d]amages are not recoverable which are not
16 causally connected with the breach.” *Pat. Scaffolding*, 64 Cal. Rptr. at 191–92. There is
17 simply no damage alleged that is causally connected with this theory of breach. Remember,
18 the only damage that X Corp. plausibly pleaded in the instant complaint is that resulting from
19 scraping and selling of data. X Corp. has not alleged *any* damage resulting from access
20 through unauthorized means, merely alluding to diminished capacity and reputational harm
21 without pleading any impairment or deprivation of servers. Again, X Corp. will be allowed to
22 seek leave to amend to allege damage (if any) resulting from access through unauthorized
23 means, as set out at the end of this order. But the instant complaint has failed to state a claim
24 for breach of contract based on such access.

25 In sum, X Corp. fails to state a claim based on access to systems. Violating X Corp.’s
26 Terms does not itself state a claim for trespass or fraud. Here, there are no allegations of
27 servers harmed or identities misrepresented. Additionally, there are no allegations of any
28 damage resulting from automated or unauthorized access, as required to state claims for

1 tortious interference with contract and breach of contract to the extent those claims are based
2 on it. This does not mean that access to systems can never support such claims, but rather that
3 no such claims have been plausibly pleaded.

4 2. CLAIMS BASED ON SCRAPING AND SELLING OF DATA.

5 To review, X Corp. seeks to redress two grievances. *First*, according to X Corp., Bright
6 Data has *improperly accessed its systems* and assisted others in improperly accessing its
7 systems. *Second*, according to X Corp., Bright Data has *improperly scraped and sold its data*,
8 and assisted others in improperly scraping its data. This order takes up the two grievances
9 separately, recognizing that some of X Corp.’s claims turn on the former (*i.e.*, trespass to
10 chattels, fraudulent violation of Section 17200), some turn on the latter (*i.e.*, misappropriation,
11 unjust enrichment), and some turn on both (*i.e.*, tortious interference with contract, breach of
12 contract). The prior section explained why the instant complaint fails to state a claim based on
13 access to systems. This section explains why it fails to state a claim based on scraping and
14 selling of data.

15 X Corp.’s interest in the data scraped and sold is fundamentally different from its interest
16 in the systems accessed. Pursuant to the Terms, X users “own [their] Content” and “retain
17 [their] rights to any Content [they] submit, post or display” on X, with “Content” broadly
18 defined as “any information, text, links, graphics, photos, audio, videos, or other materials or
19 arrangements of materials uploaded, downloaded or appearing on the Services” (Terms 3–4).
20 According to X Corp., Bright Data and its customers scrape information, text, links, graphics,
21 photos, audio, videos, or other materials or arrangements of materials that X users submit
22 (*e.g.*, “user name,” “bio”), post (*e.g.*, “comments,” “images”), and display (*e.g.*, “verified,”
23 “# of followers”) on X (*see* Amd. Compl. ¶¶ 51, 58). So, “X Corp. data” scraped and sold
24 encompasses *X users’ content*, which X users own and retain their rights in.

25 Meanwhile, X users grant X Corp. “a broad, royalty-free license to make [that] content
26 available to the rest of the world and to let others do the same” (Terms 1). Specifically, they
27 grant a “*non-exclusive*, royalty-free license” to X Corp. “to use, copy, reproduce, process,
28 adapt, modify, publish, transmit, display and distribute such Content” (Terms 3–4) (emphasis

added). As our court of appeals has explained, a non-exclusive licensee “has no more than a privilege that protects him from a claim of infringement,” and “because such a licensee has been granted rights only vis-à-vis the licensor, not vis-à-vis the world, he or she has no legal right to exclude others.” *Minden Pictures, Inc. v. John Wiley & Sons, Inc.*, 795 F.3d 997, 1004 (9th Cir. 2015). Yet that is *exactly what X Corp. seeks to do* with its claims based on scraping and selling of data — to exclude others from using, copying, reproducing, processing, adapting, modifying, publishing, transmitting, displaying, and distributing X users’ content.

Note the rights X Corp. acquires from X users under the non-exclusive license closely track the *exclusive* rights of copyright owners under the Copyright Act. The license gives X Corp. rights to reproduce and copy, to adapt and modify, and to distribute and display (Terms 3–4). Section 106 of the Act gives “the owner of copyright . . . the exclusive rights to do and to authorize any of the following”: “to reproduce . . . in copies,” “to prepare derivative works,” “to distribute copies . . . to the public by sale,” and “to display . . . publicly.” 17 U.S.C. § 106. But X Corp. disclaims ownership of X users’ content and does not acquire a right to exclude others from reproducing, adapting, distributing, and displaying it under the non-exclusive license.

So how does X Corp. purport to do this? The Terms separately state that “scraping the Services in any form, for any purpose without our prior written consent is expressly prohibited,” and that “[i]f [a user] want[s] to reproduce, modify, create derivative works, distribute, sell, transfer, publicly display, publicly perform, transmit, or otherwise use . . . Content on the Services, [they] must use the interfaces and instructions [X Corp.] provide[s] Otherwise, all such actions are strictly prohibited” (Terms 6, 8). Although X Corp. does not acquire the right to exclude others from reproducing, adapting, distributing, and displaying X users’ content under the Terms’ non-exclusive license, X Corp. ostensibly acquires that right under the Terms (*see* Amd. Compl. ¶¶ 25, 29). To the extent X Corp.’s claims are based on scraping and selling of data, they rest on these contractual provisions.⁴

⁴ For the misappropriation and unjust enrichment claims, the provisions serve to establish that Bright Data’s appropriation of data and retention of benefits were without authorization (Amd.

One might ask why X Corp. does not just acquire ownership of X users' content or grant itself an exclusive license under the Terms. That would jeopardize X Corp.'s safe harbors from civil liability for publishing third-party content. Under Section 230(c)(1) of the Communications Decency Act, social media companies are generally immune from claims based on the publication of information "provided by another information content provider." 47 U.S.C. § 230(c)(1). Meanwhile, under Section 512(a) of the Digital Millennium Copyright Act ("DMCA"), social media companies can avoid liability for copyright infringement when they "act only as 'conduits' for the transmission of information." *Columbia Pictures Indus., Inc. v. Fung*, 710 F.3d 1020, 1041 (9th Cir. 2013); 17 U.S.C. § 512(a). X Corp. wants it both ways: to keep its safe harbors yet exercise a copyright owner's right to exclude, wresting fees from those who wish to extract and copy X users' content.

The upshot is that, invoking state contract and tort law, X Corp. would entrench its own private copyright system that rivals, even conflicts with, the actual copyright system enacted by Congress. X Corp. would yank into its private domain and hold for sale information open to all, exercising a copyright owner's right to exclude where it has no such right. We are not concerned here with an arm's length contract between two sophisticated parties in which one or the other adjusts their rights and privileges under federal copyright law. We are instead concerned with a massive regime of adhesive terms imposed by X Corp. that stands to fundamentally alter the rights and privileges of the world at large (or at least hundreds of millions of alleged X users). For the reasons that follow, this order holds that X Corp.'s state-law claims against Bright Data based on scraping and selling of data are preempted by the Copyright Act.⁵

Compl. ¶¶ 90–91, 109–110). *See United States Golf Ass'n v. Arroyo Software Corp.*, 81 Cal. Rptr. 2d 708, 714 (Cal. Ct. App. 1999); *Tufeld Corp. v. Beverly Hills Gateway, L.P.*, 302 Cal. Rptr. 3d 203, 216–17 (Cal. Ct. App. 2022). For the tortious-interference and breach-of-contract claims, the provisions supply Bright Data's requisite breach and/or disruption (Amd. Compl. ¶¶ 73, 83). *See Pac. Gas & Elec.*, 791 P.2d at 589–90; *Oasis*, 250 P.3d at 1121.

⁵ In a supplemental brief, X Corp. has suggested that copyright preemption was waived because it was relegated to a passing reference in discussion of two tort claims in the motion to dismiss (Dkt. No. 64 at 1). This order disagrees. Bright Data raised the issue in its motion (Br. 20 n.13, 30

1 “A fundamental principle of the Constitution is that Congress has the power to preempt
2 state law,” deriving from the Supremacy Clause. *Crosby v. Nat’l Foreign Trade Council*,
3 530 U.S. 363, 372 (2000) (citing U.S. Const. art. VI, cl. 2). In exercise of that power, it leaves
4 state law that conflicts with federal law “without effect.” *Altria Grp, Inc., v. Good*, 555 U.S.
5 70, 76 (2008). The power to preempt “may be either expressed or implied.” *Gade v. Nat’l*
6 *Solid Wastes Mgmt. Ass’n*, 505 U.S. 88, 98 (1992).

7 Congress introduced express copyright preemption in Section 301(a) of the Copyright
8 Act of 1976. By way of background, prior to that year, our country had a “dual system” of
9 copyright protection, whereby unpublished works were protected by state “common law
10 copyright” and published works were protected by federal “statutory copyright.” H.R. Rep.
11 No. 94-1476, at 129 (1976). The Copyright Act of 1976 eliminated the dual system in favor of
12 “a single Federal system,” with Section 301(a) as a “bedrock provision[]” facilitating the
13 replacement. *Ibid.* That provision expressly preempts state-law claims when a plaintiff’s work
14 “come[s] within the subject matter of copyright” and state law grants “legal or equitable rights
15 that are equivalent to any of the exclusive rights within the general scope of copyright.”
16 17 U.S.C. § 301(a); *see, e.g., Best Carpet Values, Inc. v. Google, LLC*, 90 F.4th 962, 970–71
17 (9th Cir. 2024).

18 As recognized by our court of appeals, however, “claims are not preempted if they fall
19 outside the scope of [Section] 301(a)’s express preemption *and are not otherwise in conflict*
20 *with the Act.*” *Ryan v. Editions Ltd. W., Inc.*, 786 F.3d 754, 760 (9th Cir. 2015) (emphasis
21 added). Although conflict preemption has played second fiddle to express preemption in the
22 caselaw as of late, it is the more appropriate consideration when the question presented is not
23 whether rights created by state law are *equivalent* to rights created by federal copyright law but
24 whether enforcement of state law *undermines* federal copyright law. As legal commentators
25

26
27 n.18), expanded upon it in its reply (Reply Br. 22), applied it to all tort claims in its supplemental
28 briefing (Dkt. No. 60 at 7–12), and applied it to the breach-of-contract claim in its motion for
summary judgment (Dkt. No. 62 at 13–17). Under such circumstances, this expansion was
justified. There was no prejudice to X Corp., which briefed copyright preemption for every claim
(Dkt. No. 64 at 4–11; Dkt. No. 69 at 20–23).

1 have observed for decades, the question is often teed up where, as here, state-law claims draw
 2 upon a standard form contract. That rights created by contract law are not “equivalent” to
 3 rights created by copyright law does not mean that copyright law will never come into conflict
 4 with broad-based contractual terms.⁶

5 Conflict preemption bars state-law claims “to the extent of any conflict with a federal
 6 statute.” *Crosby*, 530 U.S. at 372. According to the Supreme Court in its latest decision
 7 concerning conflict preemption by the Copyright Act, “[n]o simple formula can capture the
 8 complexities of this determination; the conflicts which may develop between state and federal
 9 action are as varied as the fields to which congressional action may apply.” *Goldstein v.*
 10 *California*, 412 U.S. 546, 561 (1973). The Supreme Court has found conflict preemption
 11 where the enforcement of state law “stands as an obstacle to the accomplishment and execution
 12 of the full purposes and objectives of Congress.” *Crosby*, 530 U.S. at 373. “What is a
 13 sufficient obstacle is a matter of judgment, to be informed by examining the federal statute as a
 14 whole and identifying its purpose and intended effects.” *Ibid*.

15 Recall, our court of appeals has held that giving social media companies “free rein to
 16 decide, on any basis, who can collect and use data — data that the companies do not own, that
 17 they otherwise make publicly available to viewers, and that the companies themselves collect
 18 and use — risks the possible creation of information monopolies that would disserve the public
 19 interest.” *hiQ Labs*, 31 F.4th at 1202. That said, it has not yet ruled on the issue here
 20 presented. Absent a controlling decision from this circuit, this district court looked to
 21 persuasive authorities. *See, e.g., In re Jackson*, 972 F.3d 25 (2d Cir. 2020). Applying general
 22 principles, this order concludes that the extent to which public data may be freely copied from
 23

24 ⁶ *See, e.g.,* Guy A. Rub, *A Less-Formalistic Copyright Preemption*, 24 J. INTELL. PROP. L. 327,
 25 340 (2017); Jessica D. Litman & Pamela Samuelson, *The Copyright Principles Project:*
 26 *Directions for Reform*, 25 BERKELEY TECH L.J. 1175, 1238 (2010); Mark A. Lemley, *Beyond*
 27 *Preemption: The Law and Policy of Intellectual Property Licensing*, 87 CALIF. L. REV. 111, 125–
 28 26 (1999). *Cf. ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447, 1455 (7th Cir. 1996) (thinking “it
 prudent to refrain from adopting a rule that anything with the label ‘contract’ is necessarily outside
 the [express] preemption clause” and noting with approval another circuit’s “recogni[tion of] the
 possibility that some applications of the law of contract could interfere with the attainment of
 national objectives”).

1 social media platforms, even under the banner of scraping, should generally be governed by the
2 Copyright Act, not by conflicting, ubiquitous terms.

3 There are three ways in which X Corp.’s state-law claims based on scraping and selling
4 of data undermine the purpose and intended effects of the Copyright Act.

5 *First*, these state-law claims interfere with the exploitation of copyright owners’
6 exclusive rights, thereby “frustrat[ing] the operation of a provision of federal copyright law.”
7 *See id.* at 34 n.5. Section 106 of the Copyright Act empowers a copyright owner to exclude
8 others from reproducing, adapting, distributing, and displaying their copyrighted works.
9 17 U.S.C. § 106. And, Section 101 of the Act makes clear that a non-exclusive license (unlike
10 an exclusive license) does not transfer copyright ownership or any of a copyright owner’s
11 exclusive rights. *Id.* § 101. But X Corp.’s state-law claims based on scraping and selling of
12 data would empower X Corp., as a non-exclusive licensee, to exclude others from reproducing,
13 adapting, distributing, and displaying X users’ copyrighted content — even though X users
14 licensed their copyrighted content to X Corp. “to make [it] available to the rest of the world
15 and to let others do the same” (Terms 5). Consider X users who have posted their original
16 photographs on X. Under the Terms, X Corp. acquires a non-exclusive license from each of
17 those X users to reproduce, adapt, distribute, and display their original photographs. Because
18 non-exclusive licenses grant rights only vis-à-vis each copyright owner, X Corp. does not
19 acquire a legal right to exclude others from reproducing, adapting, distributing, and displaying
20 the original photographs under such licenses. *Minden*, 795 F.3d at 1004. Yet that is precisely
21 what X Corp. seeks to do.⁷

22 *Second*, X Corp.’s state-law claims based on scraping and selling of data would frustrate
23 the operation of another provision of federal copyright law by interfering with the exercise of
24 the statutory privilege of fair use. Although Section 106 gives a copyright owner exclusive
25 rights to do and to authorize the reproduction, adaptation, distribution, and display of their

26
27 ⁷ When X Corp. removes infringing content pursuant to a takedown request from a copyright
28 owner under the DMCA (*see* Terms 4), it is not interfering with the exploitation of the copyright
owner’s exclusive rights and frustrating a provision of federal copyright law because it is acting on
behalf of the copyright owner pursuant to federal copyright law. *See* 17 U.S.C. § 512(c)(3)(A)(vi).

copyrighted works, Section 107 provides for the exception that *anyone* may make fair use of copyrighted works without permission or payment of money. 17 U.S.C. § 107. This statutory privilege may or may not apply in any given instance, but in *all* instances it would be obliterated by X Corp. Only by receiving permission and paying X Corp. could Bright Data, its customers, and other X users freely reproduce, adapt, distribute, and display what might (or might not) be available for taking and selling as fair use. Thus, Bright Data, its customers, and other X users who wanted to make fair use of copyrighted content would not be able to do so. This flouts Congress’s intent that “[t]he *limited* scope of the *copyright holder’s* statutory monopoly . . . reflect[] a balance of competing claims upon the public interest.” *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 431 (1984) (emphasis added).

Third, X Corp.’s state-law claims based on scraping and selling of data “attempt[] to protect that which Congress intended to be free from restraint.” *Goldstein*, 412 U.S. at 559. Congress enacted a “scheme of carefully balanced property rights that give authors and their publishers sufficient inducements to produce and disseminate original creative works and, at the same time, allow others to draw on these works in their own creative and educational activities.” *Goldstein on Copyright* § 1.14 (3d ed. 2023). X Corp. would upend the careful balance Congress struck between what copyright owners own and do not own, and what they leave for others to draw on. In addition to giving itself de facto copyright ownership in copyrighted content that X users designated for public use, X Corp. would give itself de facto copyright ownership over content that Congress declined to extend copyright protection to in the first place (*e.g.*, likes, user names, short comments) when that content, “not ‘original’ in the constitutional sense[,] . . . may not be copyrighted.” *Feist Publications, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 347–48 (1991). This shrinks the public domain, restricting free reproduction, adaptation, distribution, and display of publicly available, non-expressive material.

“It does not follow, however, that state law [] interests are inevitably preempted whenever their recognition would burden the enjoyment of the benefits of copyright.” *In re Jackson*, 972 F.3d at 35. In evaluating whether the enforcement of state law stands as an

1 obstacle to the accomplishment and execution of the full purposes and objectives of Congress,
 2 one must consider whether a “state-created right vindicates a substantial state law interest, *i.e.*,
 3 an ‘interest[] outside the sphere of congressional concern in the [copyright] laws,’ that is
 4 ‘distinct from the interests served by the federal law which may preempt the claim[s].’” *Id.*
 5 at 37 (quoting *Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*, 489 U.S. 141, 155 (1989))
 6 (alterations in original). For example, the Copyright Act should not preempt analogous state-
 7 law claims asserted by a social media company to protect its users’ privacy because “the
 8 protection of privacy is not a function of the copyright law,” which “offers a limited monopoly
 9 to encourage ultimate public access to the creative work of the author.” *Garcia v. Google,*
 10 *Inc.*, 786 F.3d 733, 745 (9th Cir. 2015). X Corp., however, is not looking to protect X users’
 11 privacy. It contends that “improper scraping . . . interferes with *X Corp.’s own sale of its data*
 12 *through a tiered subscription service*” (Opp. 31) (emphasis added). X Corp. is happy to allow
 13 the extraction and copying of X users’ content so long as it gets paid. To the extent X Corp.’s
 14 state-law claims are based on scraping and selling of data, they “amount[] to little more than
 15 camouflage for an attempt to exercise control over the exploitation of a copyright.” *In re*
 16 *Jackson*, 972 F.3d at 38. Accordingly, to the extent X Corp.’s state-law claims are based on
 17 scraping and selling of data, they are preempted.

18 * * *

19 In closing, this order observes that X Corp. alleges one additional theory of breach that
 20 did not warrant discussion above. The Terms (now) provide that it is “a violation of these
 21 Terms to facilitate or assist others in violating these Terms, including by distributing products
 22 or services that enable or encourage violation of these Terms” (Terms 8; *see* Amd. Compl.
 23 ¶ 30). Yet, as Bright Data pointed out in its reply — and X Corp. did not contest at the hearing
 24 or in the supplemental briefing — X Corp. stuck this language into its Terms *after* it already
 25 filed an initial complaint against Bright Data alleging, *inter alia*, breach of contract (*see* Reply
 26 Br. 4 n.4 (Exhs. 4–6)). It then proceeded to file an amended complaint, enlarging its breach-
 27 of-contract claim to account for the additional theory of breach (*see* Amd. Compl. ¶¶ 70, 74).
 28 X Corp. “has not cited any case, and our research has revealed none, where a party was

permitted unilaterally to amend a contract midway through litigation concerning that contract.”
Al-Safin v. Cir. City Stores, Inc., 394 F.3d 1254, 1260 n.5 (9th Cir. 2005). No further analysis
of this theory of breach is required.

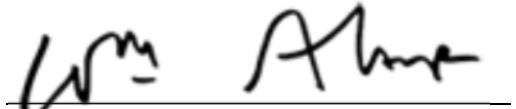
CONCLUSION

For the foregoing reasons, the motion to dismiss for failure to state a claim is **GRANTED**
and the instant complaint is **DISMISSED**. Subsequently filed motions and requests that remain
pending will be considered if and when X Corp. provides a viable complaint.

X Corp. may seek leave to amend its complaint by motion no later than **THURSDAY,**
JUNE 6, AT NOON. Any motion for leave to amend should affirmatively demonstrate how the
proposed amended complaint corrects deficiencies identified in this order as well as all other
deficiencies raised in Bright Data’s motion. It should be accompanied by a redlined copy of
the proposed amended complaint showing all proposed amendments. If X Corp. seeks leave to
amend, it must plead its best case. Otherwise, judgment will be entered.

IT IS SO ORDERED.

Dated: May 9, 2024.


WILLIAM ALSUP
UNITED STATES DISTRICT JUDGE