DAVID H. HARPER*
david.harper@haynesboon.com
JASON P. BLOOM*
jason.bloom@haynesboone.com
HAYNES AND BOONE, LLP
One Victory Park
2323 Victory Avenue, Suite 700
Dallas, Texas 75219
Telephone: (214) 651-5000
Facsimile: (214) 651-5940
**Pro hac vice to be submitted*

JASON T. LAO, SBN 288161
jason.lao@haynesboone.com
ANDREA LEVENSON, SBN 323926
andrea.levenson@haynesboone.com
HAYNES AND BOONE, LLP
600 Anton Boulevard, Suite 700
Costa Mesa, California 92626
Telephone: (949) 202-3000
Facsimile: (949) 202-3001

Attorneys for Plaintiff
X Corp.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

X CORP., a Nevada corporation,

Plaintiff,

vs.

BRIGHT DATA LTD., an Israeli corporation,

Defendant.

Case No. _____

COMPLAINT

JURY TRIAL DEMAND

Plaintiff X Corp. ("X Corp." or "Plaintiff"), by and through its undersigned counsel, hereby files its Complaint against Defendant Bright Data Ltd., ("Bright Data" or "Defendant"), and in support thereof alleges as follows:

INTRODUCTION

1. Defendant Bright Data Ltd. has built an illicit data-scraping business on the backs of innovative technology companies like X Corp., which operates the social media platform formerly known as Twitter and now known as X. Bright Data scrapes and sells millions of records from X Corp.'s X platform, in blatant violation of X Corp.'s Terms of Service, by which Bright Data is bound. Bright Data also induces and facilitates other X users to violate their own agreements with X Corp. by selling automated data-scraping tools and services that specifically target a wide range of X Corp. data.

2. Bright Data uses elaborate technical measures to evade X Corp.'s anti-scraping technology, taxing the resources of X Corp.'s servers and hampering the user experience for legitimate X users. Bright Data is aware that its activities violate X Corp.'s Terms, because the company and its executives are registered X account holders who have agreed to abide by those Terms.

3. X Corp. brings this action for injunctive relief to halt Bright Data's unauthorized use of X Corp.'s platform and for damages caused by Bright Data's breach.

THE PARTIES

4. Plaintiff X Corp. is a privately held corporation duly organized and existing under the laws of the State of Nevada with its principal place of business at 1355 Market Street, Suite 900, San Francisco, California, 94103. X Corp. owns and operates the social media platform X, formerly known as Twitter.

5. On information and belief, Defendant Bright Data was incorporated in Israel in 2008 as Zon Networks Ltd. and changed its name to Bright Data Ltd. in 2021. Bright Data has its principal place of business at 4 Hamahshev St., Netanya 4250714, in Israel. Bright Data maintains an office at L415 Mission Street, 37th Floor, in San Francisco, California.

6. Defendant Bright Data operates brightdata.com, where it sells data scraped from

numerous websites and social media platforms, including X, along with tools and services to scrape data from X and other platforms.

JURISDICTION AND VENUE

7. This Court has jurisdiction over this action under 28 U.S.C. § 1332 because complete diversity exists, and the amount in controversy exceeds $75,000. Plaintiff X Corp. is incorporated in Nevada with its principal place of business in California. Defendant Bright Data is incorporated in Israel with its principal place of business in Israel.

8. This Court has personal jurisdiction over Defendant because Defendant has consented to X Corp.'s Terms, which require all disputes related to the Terms be brought in the federal or state courts located in San Francisco, California. As part of its agreement to those Terms, Defendant also consented to personal jurisdiction in California.

9. Additionally, this Court has personal jurisdiction over Defendant because Defendant knowingly directed prohibited conduct to California. Defendant maintains a sales office in California, offers its data sets and scraping tools for sale in California, and has targeted X Corp., which has its principal place of business in California, as well as X Corp.'s users located in California.

10. Venue is proper in this district under 28 U.S.C. § 1391, because a substantial part of the events or omissions giving rise to the claims occurred in this judicial district. During all relevant times, Defendant repeatedly, knowingly, and intentionally targeted its wrongful acts at X Corp., which has its principal place of business in this district.

11. Pursuant to Civil L.R. 3-2(d), this case may be assigned to either the San Francisco or Oakland division because X Corp. is located in San Francisco County.

FACTUAL ALLEGATIONS

A. X Corp.'s Platform and Terms of Service

12. Plaintiff X Corp. owns and operates the social media platform X, accessible through twitter.com, X.com and various mobile and online applications.

13. The X platform has hundreds of millions of active users worldwide.

14. X Corp. allows its registered users to post and share content, including written

comments, images and videos, known as posts or "Tweets," and to share, like and comment on other users' posts.

15. To post content on X or to re-post, like or otherwise interact with posts by others, users must register for an account and log in to that account.

16. To register for an account, users must provide their name, phone number or email address, and date of birth. To prevent automated services from registering for accounts, X Corp. requires potential account holders to complete a "CAPTCHA" fraud-detection process to determine whether the user is human. X Corp. then verifies registrants through email or phone confirmation.

17. All users who register for a X account, and/or view the X website or application agree to form 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 Twitter Rules and Policies (collectively the "Terms").

18. X Corp.'s Terms state that a user may not "access, tamper with, or use non-public areas of the Services, our computer systems, or the technical delivery systems of our providers" or "breach or circumvent any security or authorization measures."

19. X Corp.'s Terms also state a user may not "access or search or attempt to access or search the Services by any means (automated or otherwise) other than through our currently available, published interfaces that are provided by us (and only pursuant to the applicable terms and conditions), unless you have been specifically allowed to do so in a separate agreement with us."

20. In addition, X Corp.'s Terms specifically state that "scraping the Services without our prior consent is expressly prohibited."

21. Under the Terms, users may not "forge any TCP/IP packet header or any part of the header information in any email or posting, or in any way use the Services to send altered, deceptive or false source-identifying information."

22. Users are also prohibited under the Terms from any conduct that would "interfere with, or disrupt, (or attempt to do so), the access of any user, host or network, including …

overloading, flooding, spamming … or by scripting the creation of Content in such a manner as to interfere with or create an undue burden on the Services."

23. The Terms also incorporate by reference X Corp.'s Platform Manipulation and Spam Policy (the "Policy"), which specifically prohibits "coordinated harmful activity that encourages or promotes behavior which violates the Twitter Rules." The Policy also prohibits "leveraging Twitter's open source code to circumvent remediations or platform defenses."

24. The Terms prohibit selling any content collected from the platform. Users may not "reproduce, modify, create derivative works, distribute, sell, transfer, publicly display, publicly perform, transmit, or otherwise use the Services or Content on the Services" unless otherwise authorized by the Terms or a developer agreement.

25. Advertisers on the X platform are also subject to X Corp.'s Ads Policies, which expressly state that advertisers must follow the Terms and all X Corp. Rules.

26. For developers who wish to retrieve or analyze X Corp.'s data, X Corp. offers specialized access to its Application Programming Interfaces ("APIs") through a tiered subscription service.

27. X Corp.'s Developer Agreement also limits the access of developers to X Corp.'s content. The Agreement instructs developers that they "may not exceed or circumvent rate limits, or any other limitations or restrictions described in this Policy or your agreement with Twitter, listed on the Developer Site, or communicated to you by Twitter."

Background on Data Scraping

28. Scraping is the process of using automated means to collect content or data from a website. The process involves making a request to a website's server, downloading the results and parsing them to extract the desired data. Data scrapers typically send large volumes of these requests, taxing the capacity of servers and diminishing the experience for legitimate users.

29. X Corp. utilizes a variety of technological measures to detect and prevent automated systems from scraping data from its platform, including industry standard automation prevention techniques, such as CAPTCHAs, user identification and IP rate limits and anomaly detection tools.

30. X Corp.'s registration process requires potential registrants to pass a CAPTCHA and provide a valid phone number or email address. Prior to creating the user's account, X Corp. sends a verification code to the email or phone number. Potential users must enter the verification code to create an account.

31. X Corp. also employs rate limits that cap the number of posts that may be viewed by registered users and those who access the platform without an account. Developers who use the X API are also capped in the number of posts they may post to, or pull from, the platform based on their subscription level.

32. X Corp. also utilizes anomaly detection to detect and block automated software that is attempting to access X Corp.'s platform.

Defendant Has Agreed to X Corp.'s Terms of Service

33. Defendant has expressly agreed to X Corp.'s Terms and is therefore bound by those Terms.

34. Initially, by using the X platform, Defendant, which is well aware of the Terms, agrees to be bound by them. The Terms specifically state:

> These Terms of Service ("Terms") govern your access to and use of our services, including our various websites, SMS, APIs, email notifications, applications, buttons, widgets, ads, commerce services, and our other covered services (https://help.twitter.com/rules-and-policies/twitter-services-and-corporate-affiliates) that link to these Terms (collectively, the "Services"), and any information, text, links, graphics, photos, audio, videos, or other materials or arrangements of materials uploaded, downloaded or appearing on the Services (collectively referred to as "Content"). By using the Services you agree to be bound by these Terms.

35. In addition to agreeing to the Terms by using X services, Defendant, which has maintained a registered account on X (@bright_data) since at least February 2016, expressly accepted and agreed to the Terms when registering its account. Bright Data's X account frequently posts content promoting the company's products and services.

36. Defendant's top executives are also registered X users and expressly agreed to X Corp.'s Terms when registering their accounts:

a. Bright Data's CEO, Or Lenchner, has maintained a registered account on X (@orlench) since at least December 2012 and regularly posts from that account.

b. Bright Data's CMO, Yanay Sela, has maintained a registered X account (@yanay_sela) since at least December 2014.

c. Bright Data's Managing Director for North America, Omri Orgad, has maintained a registered X account (@omri_orgad) since at least November 2011.

d. Bright Data's Vice President of Product, Erez Naveh, has maintained a registered X account (@nerez) since at least August 2009.

e. Bright Data's Global Communications Manager, Zachary Keyser, has maintained a registered X account (@KeyserZachary) since at least December 2019.

f. Bright Data's Founder, Ofer Vilenski, has maintained a registered X account (@vilenski) since at least November 2008.

37. On information and belief, several other employees and agents of Defendant involved in Defendant's data-scraping activities are also X account holders, including, by way of example, Artem Shibakov, a Bright Data software engineer who has maintained a registered X account (@ashibakow) since at least February 2013. These account holders have also expressly accepted and agreed to X Corp.'s Terms.

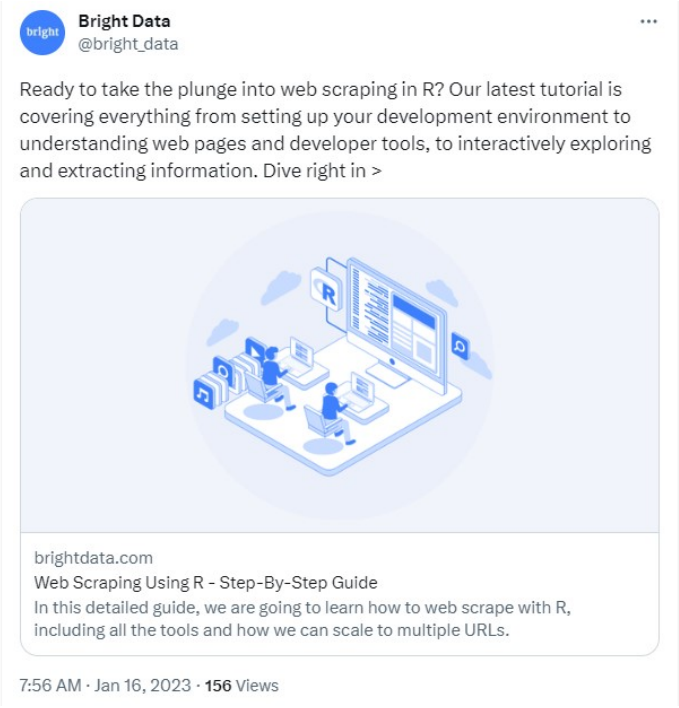
38. Defendant is additionally subject to the Terms as an advertiser on X. Beginning on March 7, 2016, Defendant (then known as Luminati Networks) purchased advertising on X. Defendant purchased additional advertising on Twitter from 2019 to 2021. As stated in X Corp.'s Ad Policies, to which Defendant expressly agreed, all advertisers are bound by the platform's Terms and Rules.

39. Defendant and its executives have repeatedly used these X accounts to discuss and promote their data-scraping products and services, including but not limited to the following posts:

a. On January 1, 2023, Defendant posted a video on X entitled "How to Scrape UNSCRAPABLE data!" which demonstrated how to use Defendant's tools and services for unauthorized data scraping.

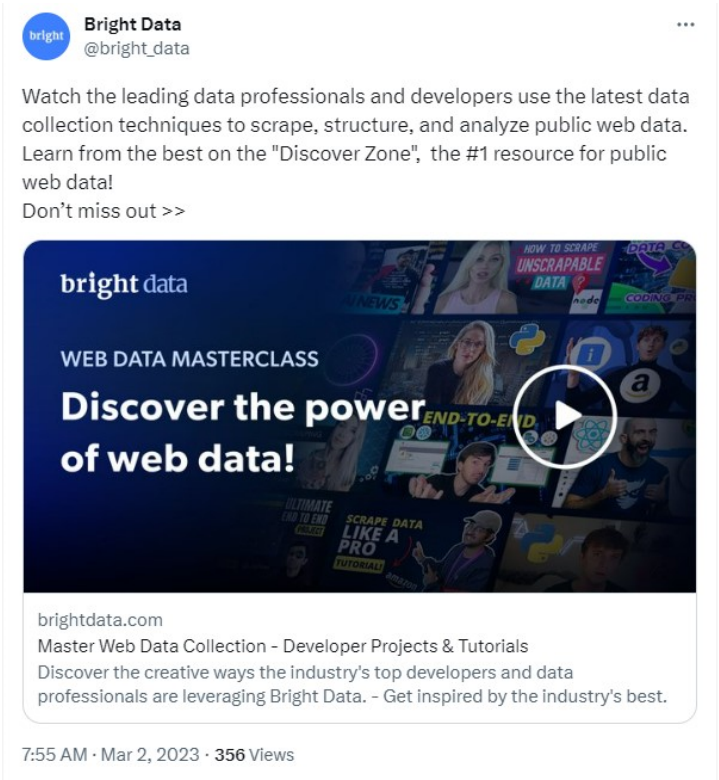
b. On January 16, 2023, Defendant encouraged users in a post on X to "take the plunge into web scraping" using a "step-by-step guide" to Defendant's tools and services.

Figure 1: Screenshot of Bright Data's website on July 11, 2023



c. On March 2, 2023, Defendant posted a video on X to a "masterclass" that showed "the latest data collection techniques to scrape, structure, and analyze public web data" using Defendant's tools and services.

Figure 2: Screenshot of Bright Data's website on July 11, 2023

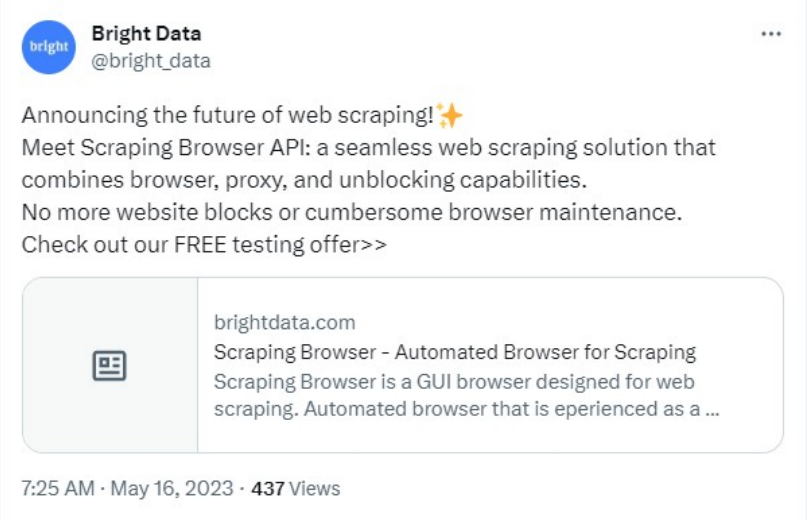


d. On March 23, 2023, Defendant posted a promoted its "Web Unblocker" and its

ability to "bypass[] multiple anti-bot solutions" in a post on X.

e. On May 16, 2023, Defendant promoted its "Scraping Browser API: a seamless web scraping solution that combines browser, proxy, and unblocking capabilities" with a link to a "FREE testing offer" in a post on X.

Figure 3: Screenshot of Bright Data's website on July 11, 2023



Defendant's Unauthorized Scraping

40. Defendant, per its own admissions, has engaged in widespread scraping of X Corp.'s data, circumventing X Corp.'s technical barriers and violating the Terms to which it agreed. Defendant has also facilitated the scraping of data from X and induced X users to violate X Corp.'s Terms.

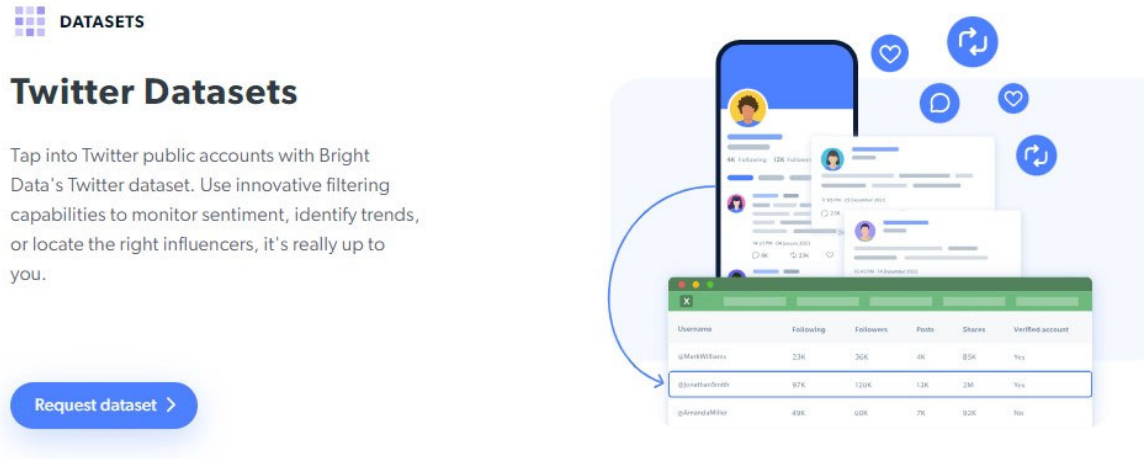
41. X Corp. has not granted Defendant permission to scrape data from the X platform.

42. Defendant has not publicly disclosed how it evades X Corp.'s technical safeguards against scraping. However, Defendant's website makes clear that the company engages in prohibited scraping on an industrial scale and brazenly advertises that Defendant sells tools and services that encourage and enable others to engage in prohibited scraping.

Defendant Scrapes and Sells Twitter Data

43. As seen in Figure 4 below, Defendant offers X Corp.'s data for sale on its website.

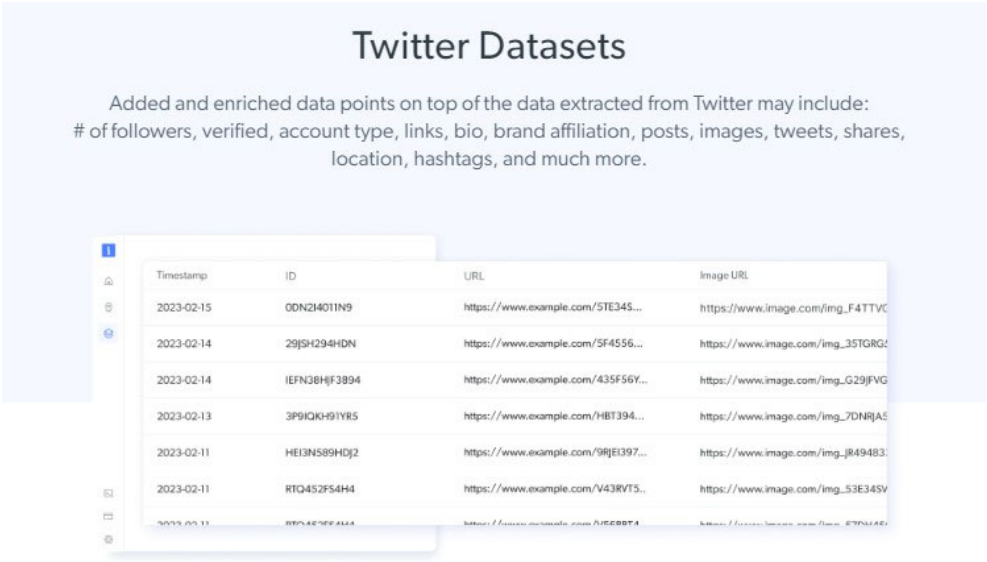
Figure 4: Screenshot of Bright Data's website on July 10, 2023



See Exh. A.

44. According to Defendant's website, the X Corp.'s data sets offered for sale by Defendant include "millions of pages and tens of millions of data points." Specifically, these data sets include the following user information: "# of followers, verified, account type, links, bio, brand affiliation, posts, images, tweets, shares, location, hashtags, and much more."

Figure 5: Screenshot of Bright Data's website on July 10, 2023



See id.

45. Defendant could have only obtained this data by engaging in prohibited scraping of X's platform.

46. Defendant offers this unlawfully obtained data for sale starting at $.01 per record,

but also offers customized packages of X Corp.'s data.

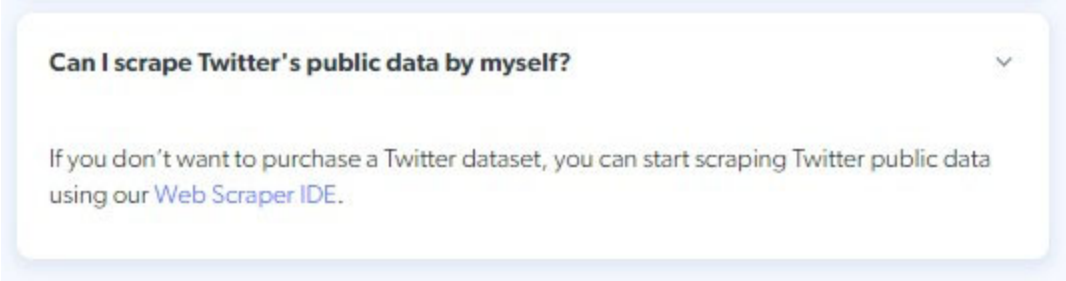
47. Defendant also offers several options for delivery of X Corp.'s data, and even offers its customers the opportunity to regularly update its data sets with additional data scraped from X at regular intervals.

Bright Data Sells Automated Tools to Scrape Twitter's Data

48. Defendant also offers for sale on its website automation software that allows users to scrape data directly from the X platform, in violation of X Corp.'s Terms.

49. As indicated in Exhibit A, Defendant's website states: "If you don't want to purchase a Twitter dataset, you can start scraping Twitter public data using our Web Scraper IDE."

Figure 6: Screenshot of Bright Data's website on July 10, 2023



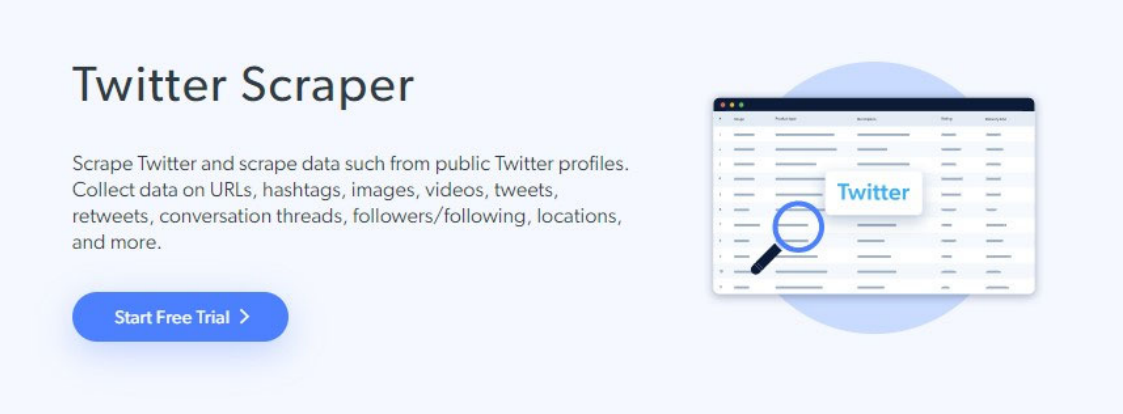
See Exh. A.

50. Defendant's Web Scraper tool allows individuals to evade detection utilizing a proxy network in order "to remain anonymous, avoid IP blocking, access geo-restricted content, and improve scraping speed." The tool also includes an "unblocking solution" that is designed to evade anti-scraping measures like those employed by X Corp. Defendant specifically advertises that its Web Scraper tool can be used to "[e]asily scrape data from any geo-location while avoiding CAPTCHAs and blocks."

51. In addition to its Web Scraper tool, Defendant sells at least four additional tools designed to scrape information specifically from the X Platform: Twitter Scraper, Twitter Profile Scraper, Twitter Image Scraper, and Twitter Followers Scraper.

a. As seen in Figure 7 below, Defendant offers a Twitter Scraper to automatically scrape data from the X platform, including "URLs, hashtags, images, videos, tweets, retweets, conversation threads, followers/following, locations, and more."

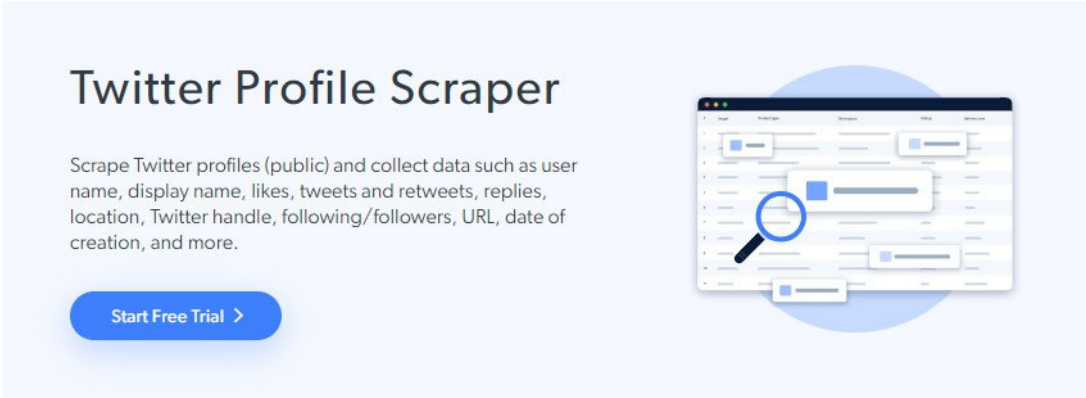
Figure 7: Screenshot of Bright Data's website on July 10, 2023



See Exh. B.

b. As seen in Figure 8 below, Defendant offers a Twitter Profile Scraper to automatically "collect data such as user name, display name, likes, tweets and retweets, replies, location, Twitter handle, following/followers, URL, date of creation, and more."

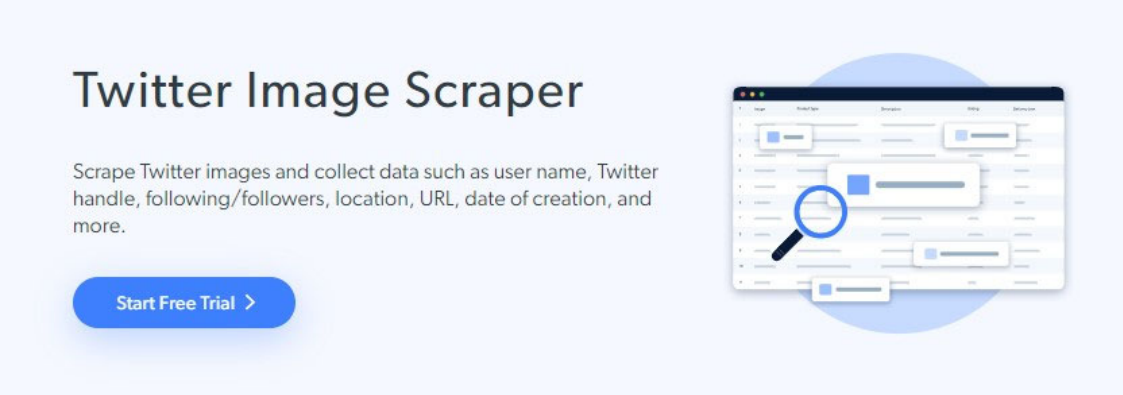
Figure 8: Screenshot of Bright Data's website on July 10, 2023



See Exh. C.

c. As seen in Figure 9 below, Defendant also offers a Twitter Image Scraper to automatically "collect data such as user name, Twitter handle, following/followers, location, URL, date of creation, and more."

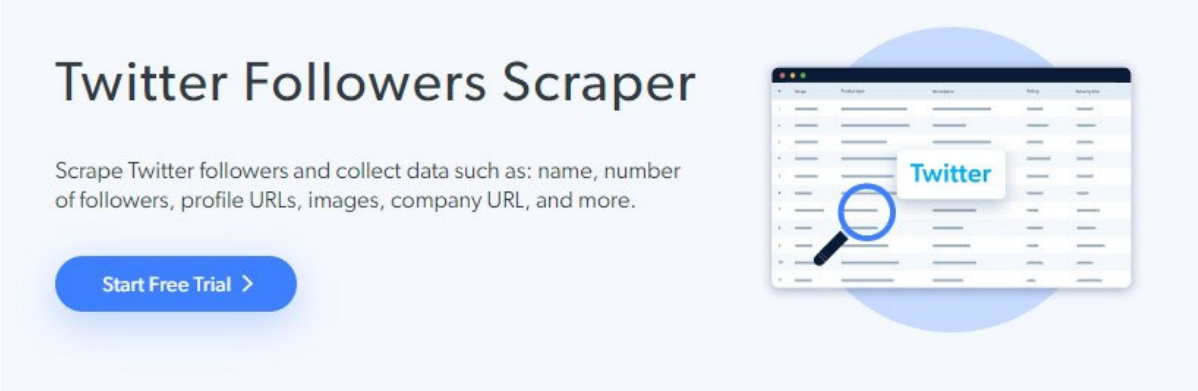
Figure 9: Screenshot of Bright Data's website on July 10, 2023



See Exh. D.

d. As seen in Figure 10 below, Defendant has also offered a Twitter Followers Scraper to automatically collect data such as "name, number of followers, profile URLs, images, company URL, and more."

Figure 10: Screenshot of Bright Data's website on July 10, 2023

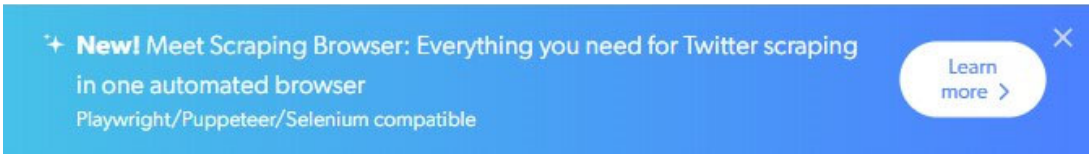


See Exh. E.

52. For each of these products, Defendant claims it "[u]tilizes proprietary technology to unlock sites" and allows customers to "collect as much data as you need quickly and completely."

53. In addition to these X-specific scraping tools, Bright Data offers an automated "Scraping Browser" that simplifies the act of scraping data from the X platform. As seen in Figure 11 below, Bright Data markets this product for scraping X Corp.'s data.

Figure 11: Screenshot of Bright Data's website on July 10, 2023



See Exh. C.

54. Defendant advertises this "Scraping Browser" as containing "all website unlocking operations under the hood, including: CAPTCHA solving, browser fingerprinting, automatic retries, selecting headers, cookies, & Javascript rendering, and more." Defendant also claims its Scraping Browser "automatically learns to bypass bot-detection systems as they adapt, saving you the hassle and cost."

55. The Scraping Browser allows Defendant's customers to "appear as a real user browser to bot-detection system[s]," such as those used by X Corp..

Bright Data Sells Proxy Services to Facilitate Data-Scraping

56. Defendant also facilitates the violation of X Corp.'s Terms by offering proxy servers specifically designed to evade anti-scraping measures, including X Corp.'s CAPTCHAs and its user ID and IP rate limits. These tools impersonate actual X users in order to bypass X Corp.'s defenses.

57. These proxy servers imitate requests from legitimate users in order to conceal the true requestor's IP address and location. Defendant advertises that these proxies will "avoid[] IP bans and CAPTCHAs" and allow users to "[g]ather vast amounts of public web data with total impunity." *See* Exhibit F.

FIRST CAUSE OF ACTION

(Breach of Contract)

58. X Corp. realleges and incorporates all preceding paragraphs herein.

59. Use of the X platform and use of X Corp.'s services are governed by X Corp.'s Terms.

60. X users, including Defendant, accept the Terms as a condition of using the platform.

61. Moreover, by virtue of having X accounts, Defendant and several of its executives,

employees, and agents have expressly accepted and agreed to X Corp.'s Terms.

62. The Terms are enforceable and binding on Defendant.

63. Defendant has repeatedly violated the Terms, including by (i) accessing the X platform through automated means without specific authorization from X Corp.; (ii) scraping data from the X platform without authorization; (iii) selling tools that allow other X users to access the X platform by automated means and to scrape data; (iv) selling proxy services that allow other X users to access the X platform by automated means and evade X Corp.'s anti-automation and anti-scraping tools; and (v) selling data that Defendant scraped from the X platform.

64. Defendant has breached and continues to breach the Terms by scraping data from X Corp.'s platform without prior consent from X Corp. X Corp. has never authorized Defendant to access its platform through automated means and has never given Defendant consent to scrape data.

65. Despite being bound by the Terms, Defendant has repeatedly accessed the X Corp. platform through automated means and scraped data in violation of the Terms.

66. Defendant has breached, and continues to breach, X Corp.'s Terms by accessing the platform through unauthorized means and scraping data from the platform.

67. Defendant has breached, and continues to breach, X Corp.'s Terms by selling tools that allow other X users to access the platform by automated means and scrape data, and by selling proxy services that allow the same.

68. Defendant has breached, and continues to breach, X Corp.'s Terms by selling data that Defendant has scraped from X Corp.'s platform.

69. Defendant's conduct has damaged X Corp. and caused and continues to cause irreparable harm and injury to X Corp.

70. X Corp. is entitled to compensatory damages, injunctive relief, declaratory relief, and/or other equitable relief.

SECOND CAUSE OF ACTION

(Tortious Interference with Contract)

71. X Corp. realleges and incorporates all preceding paragraphs herein.

72. All X users must agree to abide by the Terms, which constitute a valid and enforceable agreement between X Corp. and each user.

73. As user of X Corp.'s platform, as well as an X account holder, Defendant is aware of the Terms and that they govern all users who choose to interact with the X platform.

74. Nevertheless, Defendant has marketed and sold its scraping tools to X users and account holders, including by using the X platform to market its scraping services to other X users and account holders. Defendant has also sold proxy services and tools to facilitate automated access and scraping of the X platform.

75. By offering services and tools designed to provide automated access to the X platform, and to scrape data from the platform, Defendant induced a breach or disruption of the Terms by X users.

76. On information and belief, customers who purchased Defendant's scraping services and tools used them to access X through unauthorized, automated means and to scrape data from the X platform, in violation of the Terms.

77. Defendant's conduct has damaged X Corp. and caused and continues to cause irreparable harm and injury to X Corp.

78. X Corp. is entitled to compensatory damages, injunctive relief, declaratory relief, and/or other equitable relief.

THIRD CAUSE OF ACTION

(Unjust Enrichment, in the alternative)

79. X Corp. realleges and incorporates all preceding paragraphs herein.

80. Defendant's acts as alleged herein constitute unjust enrichment at X Corp.'s expense.

81. Defendant used X Corp.'s service, platform, and computer network without authorization to scrape data from the X platform.

82. Defendant receives benefits in the form of profits from its unauthorized scraping of X Corp. data.

83. Defendant's retention of the profits derived from its unauthorized scraping of data

would be unjust.

84. Defendants' conduct has damaged X Corp., including but not limited to hampering the user experience for authentic X users and customers, in addition to the time and money spent investigating and mitigating Defendants' unlawful conduct.

85. X Corp. seeks actual damages from Defendants' unlawful activities, an accounting, and disgorgement of Defendants' profits in an amount to be determined at trial, compensatory damages, injunctive relief, declaratory relief, and/or other equitable relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for relief, as follows:

1. Preliminary and permanent injunctive relief enjoining Bright Data, its agents, officers, employees and successors from:

a. accessing or using X Corp.'s website, servers, systems, and any data contained therein for purposes of unlawful data scaping;

b. developing or distributing any technology or product that is used, or could be used, for the unauthorized scraping of data from X;

c. facilitating the scraping of data by other users;

d. selling or offering for sale any data previously obtained from X.

2. That Defendant be required to identify the location of any and all data obtained from the X platform and to destroy any and all such data;

3. That Defendant be required to identify any and all recipients of data obtained from the X platform;

4. Compensatory, statutory, and punitive damages, as permitted by law and in such amounts to be proven at trial;

5. Reasonable costs, including reasonable attorneys' fees;

6. Pre- and post-judgment interest, as permitted by law;

7. An accounting of Defendant's profits from its scraping activities and disgorgement of those profits; and

8. Any other remedy to which Plaintiff X Corp., Inc. may be justly entitled.

Dated: July 25, 2023

Respectfully submitted,

HAYNES & BOONE LLP

By: /s/ Jason T. Lao

David H. Harper*
david.harper@haynesboone.com
Jason P. Bloom*
jason.bloom@haynesboone.com
One Victory Park
2323 Victory Avenue, Suite 700
Dallas, Texas 75219
Telephone: (214) 651.5000
Telecopier: (214) 651.5940
**Pro hac vice pending/to be submitted*

Jason T. Lao
jason.lao@haynesboone.com
Andrea Levenson
andrea.levenson@haynesboone.com
600 Anton Boulevard, Suite 700
Costa Mesa, California 92626
Telephone: (949) 202-3000
Facsimile: (949) 202-3001
Attorneys for Plaintiff X Corp.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff hereby demands a trial by jury of all triable issues.

Dated: July 25, 2023

HAYNES AND BOONE LLP

By: /s/ Jason T. Lao
Jason T. Lao