Proskauer

Court Finds hiQ Breached LinkedIn's Terms Prohibiting Scraping, but in Mixed Ruling, Declines to Grant Summary Judgment to Either Party as to Certain Key Issues

New Media and Technology Law Blog on **November 11, 2022**

On November 4, 2022, a California district court took up the parties cross-motions for summary judgment in the long-running scraping litigation involving social media site LinkedIn Corp.'s ("LinkedIn") challenge to data analytics firm hiQ Labs, Inc.'s ("hiQ") scraping of LinkedIn public profile data. (*hiQ Labs, Inc. v. LinkedIn Corp.*, No. 17-3301 (N.D. Cal. Nov. 4, 2022)). The court mostly denied both parties' motions for summary judgment on the principal scraping-related issues related to breach of contract and CFAA liability. While the court found that hiQ breached LinkedIn's User Agreement both through its own scraping of LinkedIn's site and using scraped data, and through its use of independent contractors (so-called "turkers"), who logged into LinkedIn to run quality assurance for hiQ's "people analytics" product, there were factual issues surrounding hiQ's waiver and estoppel defenses to its own scraping activities that foreclosed a judgment in favor of either party on that claim. Similarly, the court found material issues of fact which prevented a ruling on hiQ's statute of limitations defense to LinkedIn's claims under the Computer Fraud and Abuse Act (CFAA) based on emails exchanged among LinkedIn staff back in 2014 about hiQ's activities that may or may not have given LinkedIn constructive knowledge about hiQ's scraping activities and started the statute of limitations clock.

[*Note*: The court also discussed LinkedIn's requests for evidentiary sanctions based upon hiQ's alleged spoliation of and failure to preserve scraping activity records that had been stored in certain third-party cloud-based accounts, but were permanently lost after accounts became inactive. This issue is beyond the scope of this blog post.]

Most of the ink spilled covering this case has to do with the issue of the availability of the CFAA as a remedy against unwanted access to public websites. This case has been a litigation odyssey of sorts: it started with the original district court injunction in 2017, Ninth Circuit affirmance in 2019, Supreme Court vacating of the order in 2021, Ninth Circuit issuing a new order in April 2022 affirming the original injunction, and back again where we started, the lower court in August 2022 issuing an order dissolving the preliminary injunction and holding that LinkedIn had established a significant change in facts by showing that hiQ no longer had an ongoing business. What's interesting about this most recent decision is that it mainly concerns contract liability for breaching a site's user agreement and prohibitions against scraping and creating false accounts; in other scraping disputes, this type of claim is secondary to the main CFAA federal cause of action or other substantive claims. While the court did not come to a definitive answer as to liability (or delve into the amount of damages available for such a breach, which would be uncertain), the order is still instructive for both data scrapers and website operators.

As a quick recap, upon receipt of a cease and desist letter in 2017 from LinkedIn alleging, among other things, hiQ's civil liability under the CFAA, hiQ sought a preliminary injunction barring LinkedIn from blocking hiQ's access to LinkedIn public profiles. Significantly, LinkedIn sent the cease and desist letter to hiQ after years of tolerating hiQ's access and use of its data (note: hiQ's business model of employee data analysis was entirely dependent on crunching publicly available LinkedIn profile data).

Breach of contract claim

hiQ relied on LinkedIn for its data primarily by scraping public LinkedIn profiles while attempting to evade LinkedIn's technical defenses, including by hiring "turkers" who conducted quality assurance for hiQ's employee analytics product while logged-in to LinkedIn by viewing and confirming hiQ customers' employees' identities manually. When discovered by LinkedIn, the turkers resorted to creating false accounts to evade detection.

LinkedIn moved for partial summary judgment on its breach of contract claim for (1) hiQ's scraping of LinkedIn's site and using the collected data; and (2) hiQ's use of independent contractors and for directing these "turkers" to make fake accounts.

hiQ offered several defenses, including that LinkedIn's user agreement was ambiguous and unenforceable and that LinkedIn prior tolerance of hiQ's scraping constituted waiver; as for the turkers' actions, hiQ argued that they did not constitute a breach that resulted in damages and that it was not responsible for them.

LinkedIn argued that Section 8 of its User Agreement expressly prohibits scraping of its site. However, hiQ points to provisions of the User Agreement that outlines members' rights and obligations and that it considers contradictory:

2. Obligations . . . When you share information, others can see, copy and use that information.…

3.1 Your License to LinkedIn . . . . We will get your consent if we want to give others the right to publish your posts beyond the Service. However, other Members and/or Visitors may access and share your content and information, consistent with your settings and degree of connection with them.

hiQ contended that the User Agreement was ambiguous because of these supposed inconsistent provisions that prohibit scraping yet contemplate others seeing or copying profile information. The court rejected this argument, finding that contrary to hiQ's characterization, the User Agreement's provisions do not conflict with each other, as "a warning to members that a third party may collect their public-facing data is not a blessing for third parties to do so through expressly prohibited means." The court also declined to find LinkedIn's User Agreement unconscionable.

As to the turkers' conduct, hiQ argued that there was no evidence the turkers ever scraped any profile information, and generally speaking, hiQ is not responsible for its independent contractors' acts. Yet, the court noted that regardless of whether the turkers engaged in scraping, undisputed evidence showed that hiQ's turkers registered false LinkedIn identities under hiQ's instructions in breach of the User Agreement, and that "hiQ cannot escape liability because they also acted as its agent regarding the log-in process to LinkedIn."

In sum, the court found that hiQ breached LinkedIn's User Agreement both through its own scraping of LinkedIn's site and using scraped data, and through turkers' creation of false identities on LinkedIn's platform. However, it could not grant LinkedIn's motion for summary judgment for hiQ's scraping because of material facts surrounding hiQ's affirmative defenses of waiver and estoppel.

The court refused to rule as a matter of law on hiQ's waiver and estoppel defenses to LinkedIn's breach of contract counterclaim. Here, the court found a genuine dispute of material fact as to whether LinkedIn knew about hiQ's scraping and use of scraped data as early as October 2014. If it did, the court reasoned, a reasonable jury could find that LinkedIn relinquished its enforcement against hiQ's scraping through its conduct, and as noted, LinkedIn did not take specific steps beyond general anti-bot measures to legally enforce its rights against known scraping by hiQ for years, and it even allowed its employees to attend hiQ's conferences.

CFAA defense

On LinkedIn's CFAA claim, hiQ moved for summary judgment that the claim was time-barred by the statute's two-year statute of limitations. The court examined evidence of an email chain among LinkedIn employees (who were not top executives or part of the legal department) from October 2014 about an upcoming hiQ Elevate conference and musings about whether hiQ was scraping LinkedIn's site, as well as another email chain in December 2014 about a message from a venture capital investor who commented that LinkedIn likely would look unfavorably at an entity such as hiQ analyzing its member profiles. hiQ contended that these email chains showed LinkedIn had reasonable notice of hiQ's scraping more than two years before the filing of this action in 2017. LinkedIn disputed whether the employees in question had notice and, even if they did, whether their knowledge can be imputed to LinkedIn. Because more than one reasonable inference could be drawn as to whether LinkedIn knew or should have known of hiQ's scraping, the court denied hiQ's motion for summary judgment on the statute of limitations defense.

View original.

Related Professionals

- **Jeffrey D. Neuburger**