Proskauer

hiQ and LinkedIn Reach Proposed Settlement in Landmark Scraping Case

New Media and Technology Law Blog on **December 8, 2022**

On December 6, 2022, the parties in the long-running litigation between now-defunct data analytics company hiQ Labs, Inc. ("hiQ") and LinkedIn Corp. ("LinkedIn") filed a Stipulation and Proposed Consent Judgment (the "Stipulation") with the California district court, indicating that they have reached a confidential settlement agreement resolving all outstanding claims in the case.

This case has been a litigation odyssey of sorts, to the Supreme Court and back: 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 the most recent mixed ruling on November 4th, 2022. It certainly has been one of the most heavily-litigated scraping cases in recent memory and has been closely followed on our blog. Practically speaking, though, the dispute had essentially reached its logical end with the last court ruling in November – hiQ had prevailed on the Computer Fraud and Abuse Act (CFAA) "unauthorized access" issue related to public website data but was facing a ruling that it had breached LinkedIn's User Agreement due to its scraping and creation of fake accounts (subject to its equitable defenses).

The parties' settlement agreement is confidential, and the Stipulation is still subject to court approval. It is also important to note that since the conclusions set out in the Stipulation were stipulated by the parties and were not findings by the court, they are not of precedential value. Nonetheless, the Stipulation includes some notable elements:

- **Damages**: Judgment in the amount of $500,000 is entered against hiQ, with all other monetary relief waived.
- **CFAA liability**: hiQ stipulates that LinkedIn experienced losses sufficient to, and "may establish liability" under a CFAA civil claim "based on hiQ's data collection practices and based on hiQ's direct access to password-protected pages on

LinkedIn's platforms using fake accounts."

- **California "CFAA"**: hiQ stipulates that LinkedIn "may establish civil liability" under California's state-law counterpart to the CFAA based on hiQ's data collection practices, use of fake accounts and other means to evade detection by LinkedIn, hiQ's direct access to password-protected pages on LinkedIn's platforms using fake accounts, and hiQ's unauthorized commercial use of data.
- **Trespass**: hiQ stipulates that LinkedIn has established judgment as to liability under California law for the common law torts of trespass to chattels and misappropriation.
- **Irreparable harm**: hiQ stipulates that LinkedIn has established that it has suffered an irreparable injury and that LinkedIn satisfied the remaining factors and is entitled to a permanent injunction.

Injunctive Relief

The Consent Judgment also contains some broad prohibitions against hiQ's (and related parties, as defined in the Stipulation) future ability to scrape the LinkedIn platform using methods that violate the User Agreement, making no express distinction between public and non-public/password-protected portions of LinkedIn. The relief permanently enjoins hiQ from:

- **Scraping**: Scraping or accessing, whether directly or indirectly through a third party or whether logged in to a LinkedIn account or not, the LinkedIn platform in violation of its User Agreement without the express written permission of LinkedIn; creating or using fake accounts; or using the LinkedIn platform to develop a commercial service without LinkedIn's express permission.
- **Scraping software**. hiQ is immediately and permanently enjoined from developing, using, selling, or distributing any software or code "for data collection from LinkedIn platforms using any of the data, source code, or algorithms developed at hiQ" or "for analysis of data acquired from the LinkedIn platform using any of the data, source code, or algorithms developed at hiQ."
- **Deletion of code**. hiQ is required to delete any and all software or code in its possession, including code stored with third party services and source code repositories, where such code is designed "to access or interact with" or "use data acquired from" the LinkedIn platform.
- **Deletion of LinkedIn data**. hiQ must delete all LinkedIn member profile data in its possession or stored with a third party, and are similarly barred from "using, distributing, selling, analyzing, or otherwise accessing any data that hiQ collected from LinkedIn without LinkedIn's express permission, whether directly or indirectly

through a third party."

Final Considerations

It is important to note that given that the terms of the settlement do not establish any binding legal precedent, many of the questions in the case are still, to some degree, unanswered. With this litigation seemingly resolved, emerging issues with regard to web scraping and the availability of claims under the CFAA and breach of contract, among others, may be fleshed out in other venues (such as this ongoing case).

But looking back, it should be noted that this case produced the most emphatic, pro-scraping circuit court decision in technology law history when the Ninth Circuit found that hiQ "raised at least serious questions" that its scraping of public LinkedIn member profile data, even after having had its access revoked and blocked by LinkedIn, is lawful under the CFAA. Thus it will be most remembered (and cited) as speaking on the state of law concerning the availability of the CFAA as a remedy against unwanted access to public websites. The *hiQ* decisions give a green light, at least in some circumstances, to scraping publicly available websites without fear of liability under the CFAA.

Still, even removing the CFAA from the liability equation for access to public website data, we've seen that there are still potential state law claims that a site operator may bring against an unwanted data scraper. As such, the legal landscape relating to screen scraping is uncertain and the road ahead may still some rough patches.

View original.

Related Professionals

- **Jeffrey D. Neuburger**