LinkedIn Files Petition to the Supreme Court in HiQ Web Scraping Case

Article By
Jeffrey D. Neuburger
Proskauer Rose LLP
New Media and Technology Law Blog

Communications, Media & Internet
Intellectual Property
Litigation / Trial Practice
All Federal
9th Circuit (incl. bankruptcy)

Thursday, March 12, 2020

This past week, LinkedIn filed a petition for a writ of certiorari asking the Supreme Court to overturn the Ninth Circuit’s blockbuster ruling in hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985 (9th Cir. 2019). The case concerned the scope of Computer Fraud and Abuse Act (CFAA) liability associated with web scraping of publicly available social media profile data. In the appellate court ruling, the appeals court affirmed the lower court’s order granting a preliminary injunction barring LinkedIn from blocking HiQ from accessing and scraping publicly available LinkedIn member profiles. Mostly notably, the Ninth Circuit held that HiQ had shown a likelihood of success on the merits in its claim that when a computer network generally permits public access to its data, a user’s accessing that publicly available data will not constitute access “without authorization” under the CFAA. LinkedIn feels otherwise, and posed, as the question presented:

“Whether a company that deploys anonymous computer ‘bots’ to circumvent technical barriers and harvest millions of individuals’ personal data from computer servers that host public-facing websites—even after the computer servers’ owner has expressly denied permission to access the data—‘intentionally accesses a computer without authorization’ in violation of the Computer Fraud and Abuse Act.”
Even with the Ninth Circuit’s opinion, the law surrounding data scraping still remains unsettled. LinkedIn advanced several arguments as to why the Court should grant its petition and provide guidance in this area. In essence, LinkedIn declares that the hiQ decision was “unprecedented” and “denied operators of public-facing websites a critical means of protecting user data from unauthorized third-party scrapers.” Its arguments include:

- **A Circuit Split**: LinkedIn argues that there is a circuit split regarding the interpretation of the CFAA’s “unauthorized access” provision (18 U.S.C. §1030 (a)(2)) with respect to scraping. On the one hand, the Ninth Circuit has held that there is likely no CFAA violation when an outside entity scrapes data on a publicly available website, while the First Circuit in the 2003 *EF Cultural Travel* case suggested that a web scraper may act without “authorization” under the CFAA when it crawls a public website in contravention of posted terms of use containing prohibitions of scraping activities. Moreover, LinkedIn posits that a number of district courts have ruled that the CFAA applies to the unauthorized scraping of data from public-facing websites (See e.g., here and here).

“The Ninth Circuit’s decision upsets that stable understanding and prevents websites from setting and enforcing transparent standards that allow their users to understand how their data will (and will not) be used and made available to third parties.”

Given that the internet recognizes no borders, LinkedIn contends that different interpretations of the CFAA in different areas of the country is untenable.

- **The Law Was Misapplied**: LinkedIn argues that the Ninth Circuit avoided a “commonsense interpretation” of the CFAA and stressed that when it placed technical barriers to scraping its site and subsequently sent hiQ a cease and desist letter revoking permission to access the site, its further access was “without authorization.” It also contends that the Ninth Circuit’s distinction between password-protected and publicly-accessible websites is “inconsistent with the structure of the CFAA” and that if Congress had intended to limit the reach of the CFAA to non-public information it could have expressly done so.

- **The Importance of the CFAA Issue**: Because data is crucial to the digital economy, access and control are of paramount importance. Given the state of the law surrounding liability under the CFAA for unwanted scraping, LinkedIn believes that the Court could offer needed clarity.

“The issue whether public-facing websites can invoke Section 1030(a)(2) is a recurring one that is likely to arise with increasing frequency because of the critical importance of protecting the privacy of user data to citizens and website operators alike. And there is a particularly pressing need for a uniform national rule.”

LinkedIn also presents the CFAA issue as one of data privacy, stressing that when users share information on a site, it might be displayed publicly according to individual settings, but they “expect that limitations on viewing and exploiting their information will be respected” and do not envision or authorize third parties using
their data without their knowledge.

“The decision below casts aside the interests of LinkedIn members in controlling who has access to their data, the privacy of that data, and the desire to protect personal information from abuse by third parties, and it has done so in the service of hiQ’s narrow business interests. [...] Whereas LinkedIn’s privacy policy creates obligations for LinkedIn to its members and their privacy rights, third parties like hiQ can do whatever they want with member data under the Ninth Circuit’s ruling.”

Interestingly, LinkedIn doubles down on the potential privacy implications of the Ninth Circuit’s decision in invoking what is coming in the future (or what has already arrived) in terms of the potential for data misuse when scraping is combined with powerful technologies such as AI and facial recognition.

“If the Ninth Circuit’s decision is left in place, technology companies in that Circuit will have no recourse under the CFAA against, for instance, a third-party-scraper employing artificial intelligence to compile a massive database that could allow for instant facial recognition (and possible surveillance) of billions of people, while companies litigating in other circuits will be able to combat such activity.”

While open internet advocates heralded the Ninth Circuit’s decision, LinkedIn argues that allowing the Ninth Circuit’s ruling to stand may actually incentivize sites to put their networks behind a paywall or password scheme, and thus lead to the internet being less open.

“The decision below wrongly requires websites to choose between allowing free riders to abuse their users’ data and slamming the door on the benefits to their users of the Internet’s open forum.”

It is important to note that regardless of what happens on this issue, it appears that this litigation will continue as hiQ recently filed an amended complaint to, among other things, add a number of antitrust claims. Thus, the last word on all of the issues in this controversy has not yet arrived. It appears, however, that the CFAA issue might be closer to resolution. An opinion by the Supreme Court on the relationship between web scraping and the CFAA could be of enormous import. Still, if the Supreme Court declines to hear the appeal, at least in this case, on this set of facts, and in this circuit, the CFAA issue will be finally resolved.

Stay tuned!

© 2020 Proskauer Rose LLP.

Source URL: https://www.natlawreview.com/article/linkedin-files-petition-to-supreme-court-hiq-web-scraping-case