Proskauer

In Blockbuster Ruling, Ninth Circuit Affirms hiQ Injunction — CFAA Claim Likely Not Available for Scraping Publicly Available Website Data

New Media and Technology Law Blog on **September 9, 2019**

In a ruling that is being hailed as a victory for web scrapers and the open nature of publicly available website data, the Ninth Circuit today issued its long-awaited opinion in *hiQ Labs, Inc. v. LinkedIn Corp.*, No. 17-16783 (9th Cir. Sept. 9, 2019). The crucial question before the court was whether once hiQ Labs, Inc. ("HiQ") received LinkedIn Corp.'s ("LinkedIn") cease-and-desist letter demanding it stop scraping public LinkedIn profiles, any further scraping of such data was "without authorization" within the meaning of the federal Computer Fraud and Abuse Act (CFAA). The appeals court affirmed the lower court' order granting a preliminary injunction barring the professional networking platform LinkedIn from blocking HiQ, a data analytics company, from accessing and scraping publicly available LinkedIn member profiles to create competing business analytic products. Most 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.

In light of this ruling, data scrapers, content aggregators and advocates of a more open internet will certainly be emboldened, but we reiterate something we advised back in our 2017 Client Alert about the lower court *HiQ* decision: while the Ninth Circuit's decision suggests that the CFAA is not an available remedy to protect against unwanted scraping of public website data that is "presumptively open to all," entities engaged in scraping should remain careful. The road ahead, while perhaps less bumpy than before, still contains rough patches. Indeed, the Ninth Circuit cautioned that its opinion was issued only at the preliminary injunction stage and that the court did not "resolve the companies' legal dispute definitively, nor do we address all the claims and defenses they have pleaded in the district court."

Overview of the *hiQ* Dispute

Since the California district court ruling in August 2017, LinkedIn's appeal and Opening Brief in October 2017 and hiQ's subsequent Answering Brief and LinkedIn's Reply Brief, and the oral argument in March 2018, it's been a long wait for the Ninth Circuit's decision in this case. Before we dive deeper into the ruling, a brief summary the lower court proceedings is necessary.

The *hiQ* dispute involves LinkedIn's challenge to hiQ's scraping of public profile data to create a competing business analytics product. After receiving a cease-and-desist letter from LinkedIn that demanded HiQ stop its scraping activity and stated, principally, that HiQ's further access would be a violation of the federal CFAA, hiQ filed a declaratory judgment seeking a preliminary injunction barring LinkedIn from blocking hiQ's access to LinkedIn public profiles. Significantly, LinkedIn had sent the cease-and-desist letter to hiQ after years of tolerating hiQ's access and use of its data; in fact, hiQ's business model of employee data analysis at the time of the litigation was wholly dependent on crunching LinkedIn data that users elected to publish publicly. The key question concerning the applicability of the CFAA in this case was whether, by continuing to access public LinkedIn profiles after LinkedIn explicitly revoked permission to do so, hiQ had "accessed a computer without authorization" within the meaning of the CFAA.

The lower court issued a preliminary injunction, finding that the balance of equities favored *hiQ*, and distinguished the Ninth Circuit *Power Ventures* precedent that had held that a commercial entity that accesses a website after permission has been explicitly revoked can, under certain circumstances, be civilly liable under the CFAA. The lower court expressed "serious doubt" as to whether LinkedIn's revocation of permission to access the public portions of its site renders hiQ's access "without authorization" within the meaning of the CFAA. In the lower court's view, the CFAA was intended instead to deal with "hacking" or "trespass" onto private, often password-protected mainframe computers, and the district court was "reluctant" to expand its scope absent convincing authority.

On appeal, the parties offered dueling visions of what the law surrounding the CFAA and scraping should be:

- *LinkedIn*: “[A]uthorization from LinkedIn—the server’s owner—is ‘needed’ to avoid CFAA liability, regardless of whether those servers also host data that LinkedIn generally makes available on its website. hiQ lacked that required “authorization” once LinkedIn sent hiQ its cease-and-desist letter and implemented additional technological barriers restricting bot access.”
- *HiQ*: “LinkedIn does not grant permission to access its public content because those pages are, by definition, open for all to see and use. hiQ, like any other Internet user, simply requests LinkedIn’s public pages, and LinkedIn’s servers automatically provide them. There is no “authorization” for LinkedIn to revoke. Reading the statute in accordance with the language’s ordinary significance, “without authorization” refers to circumstances where authorization is a prerequisite to access.”

The CFAA Issue on Appeal

In the decision, the Ninth Circuit held that HiQ made an adequate showing at this stage to support an injunction prohibiting LinkedIn from selectively blocking hiQ’s access to public member profiles based on, among other things, the merits of its tortious interference with contract claim. While a full discussion of the merits of that claim are beyond the scope of this post, the court was compelled to consider LinkedIn’s defense that HiQ could not succeed on its tortious interference with contact and related state claims because its access to LinkedIn’s site was “unauthorized” under the CFAA. .

The pivotal CFAA question is whether once hiQ received LinkedIn’s cease-and-desist letter, any further scraping and use of LinkedIn’s data was “without authorization” within the meaning of the CFAA and thus a violation of the statute. If so, hiQ would have no legal right of access to LinkedIn’s data and so could not succeed on any of its state law claims.

Liability under the CFAA arises when a person who “intentionally accesses a computer without authorization … and thereby obtains … information from any protected computer.” 18 U.S.C. § 1030(a)(2)(C). “Without authorization” is not defined, but in the quintessential case, the CFAA is invoked to remedy incidences of computer hacking or when an employee accesses a corporate network after having had his or her permission rescinded.

In the scraping context, as seen by this highly-contested dispute, CFAA "without authorization" liability presents nuanced issues. In short, the appeals court was asked to decide whether the CFAA's "without authorization" provision is limited to computer information for which access permission, such as password authentication, is generally required.

Looking at the legislative history and precedent, the Ninth Circuit stated that the CFAA was enacted to prevent computer hacking, and that it should be best understood as "an anti-intrusion statute and not as a misappropriation statute." Thus, the court concluded that the CFAA's "without authorization" provision is "inapt" with regard to access to public LinkedIn profiles and that HiQ raised a serious question as to whether the CFAA's "without authorization" provision should only apply to computer information protected by access controls (e.g., password authentication). The Ninth Circuit distinguished its *Power Ventures* precedent, which held that that a violation of the terms of use of a website, without more, cannot be the basis for liability under the CFAA but that a social media aggregation site had accessed Facebook's computers "without authorization" after receiving an individualized cease-and-desist letter. While *Power Ventures* involved the gathering of social media user profile data protected by a username and password authentication system, the data hiQ was scraping was available to anyone with a web browser.

> "[I]t appears that the CFAA's prohibition on accessing a computer 'without authorization' is violated when a person circumvents a computer's generally applicable rules regarding access permissions, such as username and password requirements, to gain access to a computer. **It is likely 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.** [emphasis added]. The data hiQ seeks to access is not owned by LinkedIn and has not been demarcated by LinkedIn as private using such an authorization system. HiQ has therefore raised serious questions about whether LinkedIn may invoke the CFAA to preempt hiQ's possibly meritorious tortious interference claim."

Unanswered Questions and Looking Ahead

Screen or web scraping is an issue that has been controversial since the early days of e-commerce. Content aggregators and data users are always thinking of new and productive uses for data readily accessible from websites, with scraping as an obvious technical measure to access that data. Many advocate that content on publicly-available websites is implicitly free to harvest and exploit, while web services hosting valuable user-generated content or other data typically wish to exercise control over which parties can access and use it for commercial purposes. The CFAA has been one of the most potent legal tools used by website owners to challenge scraping activities. While the law surrounding screen scraping remains uncertain, the Ninth Circuit clarified whether scraping data from a public-facing website likely violates the CFAA "unauthorized access" provision, even if a website operator revokes a data scraper's access via a cease-and-desist letter.

In considering the balance of equities surrounding the lower court's grant of a preliminary injunction, the court enunciated multiple pro-scraping sentiments, echoing the lower court's concern that allowing large internet platforms to selectively restrict access to publicly available website data would not necessarily be in the public interest:

> "We agree with the district court that giving companies like LinkedIn 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."

While the *hiQ* decision is certainly a scraping-positive decision, it leaves many unanswered questions. *HiQ*, while advocating an open lane for scraping public website data, is not a complete green light for scraping in general. The Ninth Circuit held that the CFAA is likely not a viable claim for limiting the scraping of publicly available web data, yet other questions and issues are lurking:

- The calculus in any particular CFAA-scraping dispute will depend on the nature of the data at issue, as evidenced by the varying holdings in the Ninth Circuit's *Power Ventures* decision, which involved password-protected social media profiles, and *HiQ*, which involved "public" LinkedIn member data. Indeed, the *HiQ* court, in weighing whether the injunction was in the public interest, noted the nature of LinkedIn's user-generated data and implicitly differentiated it from proprietary or private data:

> "LinkedIn's asserted private business interests—'protecting its members' data and the investment made in developing its platform' and 'enforcing its User Agreements' prohibitions on automated scraping'—are relatively weak. LinkedIn has only a non-exclusive license to the data shared on its platform, not an ownership interest. Its core business model—providing a platform to share professional information—does not require prohibiting hiQ's use of that information, as evidenced by the fact that hiQ used LinkedIn data for some time before LinkedIn sent its cease-and-desist letter."

- While the crux of the decision involved the CFAA issue, LinkedIn had advanced other claims, including breach of contract, unjust enrichment and trespass to chattels. The court did not consider these claims on appeal, and noted that website operators concerned about unwanted data scraping may have causes of action beyond the CFAA, such as copyright infringement, misappropriation, breach of contract, or privacy-related claims. As we've seen in other cases involving scraping or unwanted access, such claims may be viable.
- In today's e-commerce environment, many online marketplaces scrape publicly available price data from competitors and other retailers to glean dynamic pricing and benchmarking analytics. The *HiQ* holding would appear to limit the availability of a CFAA cause of action for such activities, though, as previously discussed, other potential state causes of action remain and entities are still encouraged to follow certain risk management practices when engaged in scraping.
- While the Ninth Circuit's decisions regarding technology law are often considered persuasive authority, other jurisdictions outside of the Ninth Circuit are not bound by its decisions. Thus, the reach of the *hiQ* court's interpretation of CFAA liability for

scraping public websites is yet to be determined (and it is possible that the entire Ninth Circuit will hear the case en banc).

- What will be the practical result of the *HiQ* holding? LinkedIn and other platforms will always remain wary of "free riders" that wish to use their databases for commercial purposes. But will the decision impel LinkedIn and other similar platforms to put such data behind an authentication wall? As the court noted, many LinkedIn users intend their profiles to be accessed by other members or the public and such a radical change of access could undermine its own business model: "Of course, LinkedIn could satisfy its 'free rider' concern by eliminating the public access option, albeit at a cost to the preferences of many users and, possibly, to its own bottom line."
- Websites may still enact protective measure against malicious automated activity that threatens the integrity of their networks. The Ninth Circuit noted, in dicta, that the injunction does not preclude LinkedIn from continuing to engage in "technological self-help against bad actors."

View Original

Related Professionals

- **Jeffrey D. Neuburger**
  Partner