Taking Cue from the Supreme Court’s Van Buren Decision, Ninth Circuit Releases New Opinion Holding Scraping of Publicly Available Website Data Falls Outside of CFAA

New Media and Technology Blog on **April 21, 2022**

On remand from the U.S. Supreme Court, the Ninth Circuit earlier this week again affirmed the lower court’s order preliminarily enjoining LinkedIn Corp. (“LinkedIn”) from blocking data analytics company hiQ Labs, Inc.’s (“hiQ”) access to publicly available LinkedIn member profiles. (*hiQ Labs, Inc. v. LinkedIn Corp.*, No. 17-16783 (9th Cir. Apr. 18, 2022)) (“*hiQ II*”). In what might be considered an emphatic, pro-scraping decision (even more so than its first, now-vacated 2019 decision), the appeals court 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 federal Computer Fraud and Abuse Act (CFAA).

The panel concluded that the reasoning of last year’s Supreme Court decision in *Van Buren v. U.S.*, which interpreted the “exceeds authorized access” provision of the CFAA, reinforced the Ninth Circuit’s interpretation that the concept of “without authorization” under the CFAA does not apply to public websites. Thus, while the law relating to screen scraping remains unclear in many respects – particularly as scraping technology and the applied uses of public website data continue to evolve – this important new decision by the Ninth Circuit carries the reasoning forward from *Van Buren* and limits the applicability of the CFAA as a tool against the scraping of publicly available website data.

Last June, following *Van Buren* and the Supreme Court's separate ruling vacating and remanding the Ninth Circuit's prior decision in the *hiQ* case, we had a few questions about how the appeals court would interpret the CFAA's "without authorization" provision on remand in light of the so-called "gates up or down" approach to the CFAA espoused by the Supreme Court in *Van Buren*. In particular, we were waiting to see whether the appeals court would consider a website owner's technical measures to selectively block a specific entity's access to public website data as effectively bringing crashing down the "gates" of authorized access (and, with it, potential CFAA liability). The long wait is over and the Ninth Circuit has answered these questions with its pro-scraping, open web interpretation of the CFAA (with respect to public websites). While some additional legal questions remain unanswered in this case, it appears the CFAA "without authorization" issue has been firmly resolved, at least as far as the Ninth Circuit is concerned.

However, though one issue may has been resolved, others remain. As stated in our 2017 Client Alert about the lower court's *hiQ* decision, entities engaged in scraping should still tread carefully. As the Ninth Circuit itself says in *hiQ II*: "Entities that view themselves as victims of data scraping are not without resort, even if the CFAA does not apply."

Also, of course, this litigation does not involve the also-controversial practice of scraping mobile applications. Because the methodology involved in that type of scraping is significantly different, it is possible that a court could come to a different conclusion with respect to the CFAA in that circumstance.

Quick Recap

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, among other things, 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. 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.

Here's a brief timeline of the litigation:

August 2017: A California district court issued a ruling preliminarily enjoining LinkedIn from denying hiQ's access to publicly available member profiles on LinkedIn, finding that even after hiQ continued to access public LinkedIn profiles after LinkedIn explicitly revoked permission to do so, hiQ had not likely "accessed a computer without authorization" within the meaning of the CFAA.

September 2019: A Ninth Circuit panel ("*hiQ I*") affirmed the lower court's order granting a preliminary injunction. Most notably, in *hiQ I* 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.

June 2021: The Supreme Court granted LinkedIn’s petition for certiorari and subsequently vacated the *hiQ I* opinion and remanded the case to the Ninth Circuit for further consideration in light of the Supreme Court’s decision in *Van Buren v. United States*, 141 S. Ct. 1648 (2021). In *Van Buren*, the Court held that the CFAA’s “exceeds authorized access” provision covers those who obtain information from computer networks or databases to which their computer access does not extend and “does not cover those who, like Van Buren, have improper motives for obtaining information that is otherwise available to them.” In the decision’s most cited metaphor, the court’s view of the CFAA anti-hacking statute as a whole (including the “without authorization” provision at issue in the *hiQ* case) suggests a “gates-up-or-down” approach where the CFAA prohibits accessing data one is not authorized to access. As the Supreme Court stated: “Van Buren’s account of [the relevant CFAA provisions] makes sense of the statutory structure because it treats the ‘without authorization’ and ‘exceeds authorized access’ clauses consistently. Under Van Buren’s reading, liability under both clauses stems from a gates-up-or-down inquiry—one either can or cannot access a computer system, and one either can or cannot access certain areas within the system. And reading both clauses to adopt a gates-up-or-down approach aligns with the computer-context understanding of access as entry.”

April 2022: Having concluded that *Van Buren* reinforced its reasoning in the vacated *hiQ I* decision, the Ninth Circuit this time around again affirmed the lower court’s preliminary injunction in hiQ’s favor and ruled that hiQ raised serious questions about whether LinkedIn may invoke the CFAA to preempt hiQ’s claims or block access and, on a whole, whether hiQ’s activities are lawful under the CFAA.

[*Note*: While there are other notable facets of the *hiQ II* decision, including the court’s treatment of the merits of hiQ’s tortious interference with contract state claim, and LinkedIn’s “legitimate business purpose” defense, and the court’s balancing of the preliminary injunction factors, this post will principally focus on the CFAA and data scraping issue].

Merits of the CFAA Issue

In this case, the court looked to whether hiQ’s further scraping and use of LinkedIn’s data after having its access revoked was likely “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 LinkedIn could invoke the CFAA to preempt hiQ’s possibly meritorious tortious interference claim.

In the scraping context, as seen by this highly-contested dispute, CFAA “without authorization” liability presents nuanced issues. Here, the Ninth Circuit concluded that hiQ raised a serious question as to whether the CFAA “without authorization” concept is inapplicable where “prior authorization is not generally required but a particular person—or bot—is refused access.” In so holding, the appeals court stated that hiQ has raised a serious question as to whether the reference to access “without authorization” limits the scope of the statutory coverage to computers for which authorization or access permission, such as password authentication, is generally required. The court stated that, consistent with its prior decisions on the scope of the CFAA, “where access is open to the general public, the CFAA ‘without authorization’ concept is inapplicable.”

The Supreme Court’s *Van Buren* CFAA decision further buttressed this pro-scraping holding and was deemed consistent with Ninth Circuit CFAA precedent, even though *Van Buren* did not directly address the CFAA’s “without authorization” clause. Citing *Van Buren*, the Ninth Circuit stated that liability under both clauses of the CFAA (i.e., “exceeds authorized access” and “without authorization”) stems from the Supreme Court’s “gates-up-or-down” inquiry, as “one either can or cannot access a computer system, and one either can or cannot access certain areas within the system.”

Using *Van Buren* as a guide, the Ninth Circuit elaborated on the structure of the CFAA:

> “The CFAA contemplates the existence of three kinds of computer systems: (1) computers for which access is open to the general public and permission is not required, (2) computers for which authorization is required and has been given, and (3) computers for which authorization is required but has not been given (or, in the case of the prohibition on exceeding authorized access, has not been given for the part of the system accessed). Public LinkedIn profiles, available to anyone with an Internet connection, fall into the first category. **With regard to websites made freely accessible on the Internet, the “breaking and entering” analogue invoked so frequently during congressional consideration has no application, and the concept of “without authorization” is inapt.**” [emphasis added]

Looking to this breakdown of how the CFAA covers different types of computer systems (and their access protections), the Ninth Circuit stated that “*Van Buren*’s ‘gates-up-or-down inquiry’ is consistent with our interpretation of the CFAA as contemplating three categories of computer systems.”

> “The Court’s ‘gates-up-or-down inquiry’ thus applies to the latter two categories of computers we have identified: if authorization is required and has been given, the gates are up; if authorization is required and has *not* been given, the gates are down. As we have noted, however, a defining feature of public websites is that their publicly available sections lack limitations on access; instead, those sections are open to anyone with a web browser. **In other words, applying the ‘gates’ analogy to a computer hosting publicly available webpages, that computer has erected no gates to lift or lower in the first place**. ***Van Buren* therefore reinforces our conclusion that the concept of ‘without authorization’ does not apply to public websites.**” [emphasis added]

Further Thoughts

- **Limits of the hiQ II decision**. At the outset, it should be noted that as sweeping as the *hiQ II* decision reads, it has certain limitations. The decision concerns an affirmance of a preliminary injunction, as opposed to a ruling on the full merits at the summary judgment level; thus, at this stage, the court did not resolve the parties’ legal dispute definitively, nor address all the claims and defenses pleaded in the district court. Also, while this case was decided in the Ninth Circuit, which is the venue of many technology law (and scraping) disputes, it is not binding precedent on other circuit courts. In addition, the facts of this case concern public website member profiles on a social media site, but a future case could involve non-user data on a different type of website, database or mobile app and governed by different levels of access controls.

- **Do technical measures lower the authorization “gate”?** In our post following the Supreme Court’s *Van Buren* decision, we pondered how future courts would apply *Van Buren* in scraping cases. In the *Van Buren* case, the question of authorization and access was more or less clear-cut (a law enforcement officer was authorized to access a police database, but did so for improper motives), but in many scraping disputes, such issues can be muddy, particularly when technological measures are in play. For example, we wondered how would a court rule on the issue of whether a data scraper exceeded authorized access if it bypassed IP address blocks or other technical measures – in essence, are those measures more like authorization “gates” or more like use-related policies?

In *hiQ II*, the Ninth Circuit leaned more to the idea that authorization is only required for password-protected sites or “sites that otherwise prevent the general public from viewing the information.”

> “In recognizing that the CFAA is best understood as an anti-intrusion statute and not as a ‘misappropriation statute,’ [in prior cases] we rejected the contract-based interpretation of the CFAA’s ‘without authorization’ provision adopted by some of our sister circuits.” [citations omitted]

Here, in the *hiQ* case, the appeals court found that the public LinkedIn member profiles were information “presumptively open to all comers” and thus, using the Supreme Court’s parlance, the “gate” was up. Still, in a different situation, technical measures that apply to all users, even something different than password protection, could be employed that prevents the general public, as opposed to merely a single entity, from accessing a site (or part of a site) and might look more like a closed gate. Indeed, it was the open nature of LinkedIn’s public member profiles (and the fact that it was user data, not owned by LinkedIn, and posted publicly according to a user’s own choice) that drove the court’s reasoning on the CFAA issue in this case.

As the Ninth Circuit summed up:

> "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. 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."

- **Can a site operator still use the CFAA in an unwanted scraping situation?** At several points in the opinion, the court noted how LinkedIn had "selectively" blocked hiQ's bots and access to public member profiles. As the court stated, LinkedIn could choose to put an end to what it deemed "free riders" that scrape its public member profile data by simply eliminating the public access option to its site, a choice that the court surmised would run counter to user's preferences and perhaps the site's profitability. Many other websites would likely decline to wall off the public's access too, even if putting up authentication walls for every visitor would give sites the cudgel of the CFAA in preventing unwanted access. Still, even if many areas of a site are open to the public, computers and servers hosting public websites may contain areas that require authorization to access. As such, the Ninth Circuit stated that "[a]ccessing those areas 'without authorization' would violate the CFAA."

Moreover, the *hiQ II* court distinguished place prior Ninth Circuit decisions that applied the CFAA to instances of unwanted access. In those prior cases that affirmed CFAA liability, the unwanted scraping or access to a protected database involved data protected by username and password authentication systems, in contrast to the data hiQ was scraping, which was available to anyone with a web browser. With respect to the prior cases involving password-protected data, the court was clear ("As to the computers at issue in those cases, the authorization gate was 'down'").

Lastly, the appeals court noted that internet companies and the public have a "substantial interest in thwarting denial-of-service attacks and blocking abusive users, identity thieves, and other ill-intentioned actors," and such circumstances could perhaps justify an injunction securing even public parts of its website from malicious actors (though, such considerations were not present in *hiQ*).

The *hiQ II* decision might seem like a green light for scraping public websites, but an unsettled landscape remains.

Even removing CFAA from the liability equation for access to public website data, there are potential state law claims that a site operator may bring against an unwanted data scraper, such as breach of contract (as many website terms of use prohibit certain types of automated access such as scraping), common law trespass, copyright infringement, misappropriation, unjust enrichment, conversion, and privacy-related claims. The court noted, for example, that LinkedIn has asserted claims under the Digital Millennium Copyright Act and under trespass and misappropriation doctrines. In dicta, the Ninth Circuit even appeared open to the merits of a trespass to chattels claims if LinkedIn could show demonstrable harm. Considerations of LinkedIn's other remaining claims are still proceeding in the lower court (which could have ramifications for future cases involving public website data). Thus, even though the path for data scraping involving public websites may have cleared considerably with respect to the CFAA, it is by no means an open road, and still involves certain risks that require diligence and calculated legal and business decisions.

View Original

Related Professionals

- **Jeffrey D. Neuburger**
  Partner