LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

What 9th Circ.'s CFAA Decision Means For Data Scraping

By **Christopher Cole** (May 2, 2022, 5:38 PM EDT)

Christopher Cole

In a highly anticipated decision on remand from the U.S. Supreme Court, the U.S. Court of Appeals for the Ninth Circuit affirmed an earlier injunction in favor of hiQ Labs Inc., a data analytics firm, preventing LinkedIn Corp. from barring hiQ's scraping of LinkedIn user data.

The decision, in HiQ Labs v. LinkedIn, is the latest milestone that narrows application of the Computer Fraud and Abuse Act, which has frequently been cited in support of prohibiting data-scraping activities.

The court's decision has important ramifications for any social media platform, content provider or online retailer subject to data scraping by third parties seeking to aggregate and monetize their content.

Background

LinkedIn operates a hugely successful social media platform for professionals. LinkedIn users provide extensive information regarding their professional positions, relationships and interests, while agreeing to make their user profiles publicly available, with some user-selected limitations. It boasts of having 810 million users, making it by far the largest such professional social media site and an unparalleled source of information regarding professional relationships.

hiQ is a data analytics company that has fashioned a business of scraping professional information from LinkedIn, including profiles, work histories and skills of LinkedIn users. It conducts so-called people analytics on this information, which it then sells to its business clients.

The case began shortly after LinkedIn sent hiQ a cease and desist letter, demanding that hiQ stop scraping LinkedIn. Perceiving this to be an existential threat, hiQ sued LinkedIn for an injunction preventing LinkedIn from blocking hiQ's access to the site.

The procedural history is lengthy. The U.S. District for the Northern District of California initially granted a preliminary injunction to hiQ in 2019. The Ninth Circuit affirmed. The Supreme Court then granted certiorari, ultimately vacating the panel decision and remanding it for further consideration in light of the Supreme Court's 2021 opinion in Van Buren v. U.S.[1] In the most recent decision, on remand, the Ninth Circuit once again affirmed.

The Ninth Circuit Decision

The Ninth Circuit concluded that hiQ had met its preliminary injunction standards primarily for two reasons. First, the court concluded that the potential harm to hiQ of denying the injunction would be very large, while granting the injunction would be less harmful to LinkedIn. Second, it concluded that hiQ had presented what the court concluded were "serious questions going to the merits."

The most interesting part of the opinion revolves around the court's analysis of one of several legal theories often asserted against such data-scraping activities — the interplay between state law tortious interference claims and the federal Computer Fraud and Abuse Act.

The CFAA states in relevant part that "[w]hoever … intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains … information from any protected computer … shall be punished" by fine or imprisonment.[2]

The key question addressed by the court was whether hiQ's scraping of LinkedIn data constituted access without authorization, either before or after LinkedIn had sent the cease and desist letter, and therefore whether hiQ's tortious interference claims were preempted by the CFAA.

In concluding that hiQ's access was not without authorization, and therefore that the CFAA did not preempt state law, the court observed that the LinkedIn content hiQ had been scraping was otherwise freely available from LinkedIn to any third party with a web browser. It analogized the CFAA to a law that prevents breaking and entering, or hacking, which makes it an anti-intrusion statute.

The court concluded that authorization under the CFAA is "only required for password-protected sites or sites that otherwise prevent the general public from viewing the information." When one enters without authorization, one is hacking or entering without permission.

The court reasoned that this holding could be reconciled with the Supreme Court's recent Van Buren decision. In that case, the Supreme Court vacated the CFAA conviction of a police officer who had accepted bribes to run license plate searches using the computer in his police car. While the officer had been granted access to the license plate search system for legitimate policing work, he was prohibited from using that system to run searches unrelated to policing.

The court found that the misuse of a computer system, to which the defendant otherwise had been given access, could not give rise to a criminal CFAA conviction. Applying what it called a gates-up-or-down inquiry, the court concluded that if the defendant had access to the system already, he could not be prosecuted under the CFAA for accessing other areas of the system even if he had been told not to do so.

In the view of the court, the CFAA only criminalized unauthorized access in gates-down circumstances. Merely breaching a contractual prohibition or exceeding a code-based limitation was not without authorization within the meaning of the CFAA.

Implications

The hiQ case will likely proceed in one of two directions — either to a trial, or another trip to the Supreme Court. Therefore, it may be premature to draw definitive conclusions about the state of the law in this area — even in the Ninth Circuit.

In addition, the Ninth Circuit made a few tantalizing references to other theories that might still be asserted by LinkedIn, such as common law trespass to chattels; the fact that hiQ's contracts with third parties may be illegal; that LinkedIn has a legitimate interest in protecting the privacy of its users; and theories of copyright infringement, misappropriation, conversion and breach of contract. Clearly, LinkedIn has many arrows in its quiver.

Therefore, the decision may not be the last word on scraping and the law is still evolving. However, the decision does suggest that the CFAA is being judicially narrowed and may not represent the broad cudgel against every conceivable unauthorized access that some have asserted it to be.

In particular, plaintiffs who have relied on the CFAA to assert claims against entities that have been given access, based on the theory that the scope of their access permissions were exceeded, may have to find alternative theories of liability. Alternatively, one might expect technological solutions that involve installing new gates — a tradeoff between convenience and the facilitation of mass data gathering.

Christopher A. Cole is a partner at Crowell & Moring LLP.

[1] 141 S.Ct. 1648 (2021).

[2] 18 U.S.C. §1030(a)(2)(C).