Lowenstein Sandler

Client Alert

Investment Management

September 16, 2019

Is the Internet Public? A Review of the Ninth Circuit's Decision in *hiQ Labs, Inc. v. LinkedIn Corporation*[1]

By Peter D. Greene, Benjamin E. Kozinn, and Robert J. Menendez

What You Need To Know:

- **U.S. Court of Appeals for the Ninth Circuit rules in favor of hiQ in its web scraping dispute with LinkedIn.**
- **The Ninth Circuit ruled that data scraped from a website that could be obtained by anyone with an internet connection and a web browser is "public," and, therefore, does not violate the Computer Fraud and Abuse Act.**
- **Ruling provides helpful guidance to fund managers in assessing material, non-public information risks in utilizing web scraped data as part of their investment research processes.**

The U.S. Court of Appeals for the Ninth Circuit recently issued its long-awaited ruling in *hiQ Labs, Inc. ("hiQ") v. LinkedIn Corporation ("LinkedIn")*. The Ninth Circuit ruled that LinkedIn cannot prevent hiQ from scraping[2] the profiles of LinkedIn's members if those profiles are "available for viewing by anyone with a web browser."

This case has been closely watched by investment advisers that scrape web data (and vendors that supply web-scraped data to investment managers), as the lower court's ruling was the first significant federal or state court ruling specifically addressing the validity of web scraping and whether information on a website is considered "public."

For investors who employ web-scraped data as part of their investment research process, guidance on whether website information is public or private is of critical importance. Under U.S. securities laws, an investor cannot be found guilty of insider trading if the government cannot prove that the information it possessed was nonpublic. Although the *hiQ* case has nothing to do with insider trading, the Ninth Circuit's decision provides investors with "first-of-its-kind" legal guidance on whether information on the internet (whether scraped or simply viewed with a browser) is public or nonpublic. The Ninth Circuit concluded that information on a website is part of the public domain, and thus freely accessible by users and scrapers alike (*i.e.*, publicly available information), so long as it (i) is not demarcated as private or (ii) does not require a username, password, or other form of authentication in order to access it.

Background

HiQ is a data analytics company that uses information it scrapes from public LinkedIn profiles to provide its clients with insights on their workforces. In analyzing the facts of the case, the Ninth Circuit recognized that hiQ's business relies on access to publicly available data provided by LinkedIn members. While hiQ had been scraping LinkedIn's website for years, in 2017, LinkedIn sent hiQ a cease-and-desist letter demanding that hiQ stop scraping data from its website. LinkedIn also implemented technological barriers to block hiQ from accessing

[1] A copy of the Ninth Circuit's opinion is available at http://cdn.ca9.uscourts.gov/datastore/opinions/2019/09/09/17-16783.pdf.
[2] The court used the following definition of web scraping: "Scraping involves extracting data from a website and copying it into a structured format, allowing for data manipulation or analysis. Scraping can be done manually, but as in this case, it is typically done by a web robot or 'bot.'"

any portion of LinkedIn's website (regardless of whether a LinkedIn member's profile was otherwise viewable by anyone with a browser and internet connection). After some legal maneuvering by both parties, hiQ was ultimately granted injunctive relief by the U.S. District Court for the Northern District of California, and LinkedIn appealed to the Ninth Circuit.

Analysis

The Ninth Circuit panel analyzed most of LinkedIn's arguments through the prism of whether the information being scraped by hiQ was public or nonpublic, as the key federal statute in question, the Computer Fraud and Abuse Act, as amended (the "CFAA"), cannot be violated if, according to the court, the information being scraped by hiQ was in the public domain. The court explored the meaning of "without authorization" set forth in the CFAA, and concluded that for hiQ's scraping activity to violate the CFAA, it must be analogous to "breaking and entering" private property.

As part of its analysis, the court highlighted that "LinkedIn specifically disclaims ownership of the information users post to their personal profile," and "has no protected property interest in the data contributed by its users, as the users retain ownership over their profiles." The court also emphasized that while LinkedIn provides its members with a variety of privacy settings, this case dealt only with LinkedIn member profiles made visible to "anyone with a web browser" and internet connection. Further, in making a determination as to what is "private" on the internet, the court noted that warnings, encryptions, permissions, and passwords are usually strong indicia of private property and that "*an authentication requirement, such as a password gate, is needed to create the necessary barrier that divides open spaces from closed spaces on the Web.*" Finally, by looking at CFAA's legislative history, the court stated that a "person may reasonably conclude that a communication is readily accessible to the general public if the . . . means of access are widely known, and if a person does not, in the course of gaining access, encounter any warnings, encryptions, password requests, or other indicia of intended privacy." The court concluded that "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."

Conclusion

The court's decision is narrow in that it deals only with the scraping of the portion of a website containing information clearly available to the public. The ruling is applicable only to the federal courts located in the Ninth Circuit, and LinkedIn may further appeal the case to the U.S. Supreme Court. Nonetheless, the court's ruling affirms the view that portions of a website freely accessible by anyone with a web browser and internet connection are part of the public domain. For fund managers using scraped data as part of their "mosaic" of information, the court's ruling is an encouraging step in providing more certainty around the legal risks faced when using web-scraped data, including those related to insider trading.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

PETER D. GREENE
Partner
T: 646.414.6908
pgreene@lowenstein.com

BENJAMIN E. KOZINN
Partner
T: 212.419.5870
bkozinn@lowenstein.com

ROBERT J. MENENDEZ
Counsel
T: 212.419.5847
rmenendez@lowenstein.com