

The Tech Group White Collar Criminal Defense

June 15, 2021

Supreme Court Grants Certiorari in Web Scraping Case hiQ v. LinkedIn

By Mark P. Kesslen, Kathleen A. McGee, and Bryan Sterba

On June 14, the United States Supreme Court issued a summary disposition in hiQ Labs, Inc. v. LinkedIn Corp. ranting certiorari, vacating the Ninth Circuit's previous judgment, and remanding the case for additional consideration in light of the high court's ruling in Van Buren v. United States. The Van Buren ruling was issued less than two weeks ago and limited the reach of the Computer Fraud and Abuse Act (CFAA).2

The data analytics company hiQ relies on access to publicly available data provided by LinkedIn members to conduct its business. In 2017, LinkedIn sent hiQ a letter demanding hiQ cease and desist scraping data from LinkedIn. Additionally, LinkedIn began blocking hiQ's access and ability to scrape data from public LinkedIn profiles. After the U.S. District Court for the Northern District of California granted hiQ injunctive relief, LinkedIn appealed to the Ninth Circuit, which ruled that LinkedIn could not block hiQ from scraping data viewable to the general public.

While the Ninth Circuit's ruling may be considered beyond its jurisdiction, a definitive U.S. Supreme Court ruling regarding the merits of LinkedIn's claims (and the legality of data scraping generally) would be binding precedent for all lower courts throughout the country. Given the increased prevalence of data scraping across industries for analytic purposes, such a ruling would have a sweeping impact felt by many businesses. LinkedIn's previous discovery that

an archive of 500 million of its users' profiles had been scraped and posted for sale on the internet illustrates the impact data scraping can have on businesses like theirs.3

In its petition for certiorari, LinkedIn argued that although certain profile data is publicly available, hiQ's software bots harvest data on a larger scale than any human could.4 Further, LinkedIn argued that although the decision in Van Buren provided certainty around the reach of the CFAA when a potential violator has "exceeded" their authorized access, the high court did not provide clarity on whether a CFAA violation may occur when the potential violator has no access authorization at all.

It is possible that the high court views this as an opportunity to distinguish between exceeding authorized access and a private company's ability to deny access altogether. Many are watching this case, and a definitive decision will likely reshape the landscape of data scraping.

https://www.supremecourt.gov/orders/courtorders/061421zor_6j36.pdf

² https://www.supremecourt.gov/opinions/20pdf/19-783_k53l.pdf

https://www.reuters.com/technology/linkedin-says-some-user-data-extracted-posted-sale-2021-04-09/https://www.supremecourt.gov/DocketPDF/19/19-1116/147933/20200716141411953_19-1116 - Cert Reply.pdf

Contacts

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

MARK P. KESSLEN

Partner Chair, Intellectual Property section of The Tech Group Chair, IP Litigation Group

T: 646.414.6793 / 973.597.2330 mkesslen@lowenstein.com

KATHLEEN A. MCGEE

Partner

T: 646.414.6831 kmcgee@lowenstein.com

BRYAN STERBA

Counsel

T: 973.597.2386

bsterba@lowenstein.com

NEW YORK PALO ALTO NEW JERSEY UTAH WASHINGTON, D.C.

This Alert has been prepared by Lowenstein Sandler LLP to provide information on recent legal developments of interest to our readers. It is not intended to provide legal advice for a specific situation or to create an attorney-client relationship. Lowenstein Sandler assumes no responsibility to update the Alert based upon events subsequent to the date of its publication, such as new legislation, regulations and judicial decisions. You should consult with counsel to determine applicable legal requirements in a specific fact situation. Attorney Advertising.