Alert
Intellectual Property/Media

Weil

June 16, 2021

Scraping Suit Stymied after *Van Buren*

By Randi Singer and Michael Goodyear

On June 14, 2021, the U.S. Supreme Court granted certiorari in *LinkedIn Corp. v. hiQ Labs, Inc.*, one of the most significant Circuit-level decisions to date on the practice of data scraping. In light of the Court's recent holding in *Van Buren v. United States*, which curbed the extent of the Computer Fraud and Abuse Act ("CFAA"), the Supreme Court vacated the Ninth Circuit's opinion in *hiQ* and remanded the case for reconsideration.[1] Given the prominent role the CFAA plays in companies' efforts to halt data scraping, the Supreme Court's decisions in *Van Buren* and *hiQ* could thus cause a significant shift in future litigation targeting the practice.

The Opinion in *LinkedIn v. hiQ*

Data scraping is the extraction of online data for various purposes, from archiving data to following trends in restaurant reservations or inventory levels to staying abreast of competitors' prices. For example, hiQ Labs used automated bots to scrape employment information from public profiles on LinkedIn (including when such profiles were updated, potentially signaling a new job search) in order to generate "people analytics," which it sold to its clients. In response, LinkedIn took steps to prohibit such behavior, including by employing a text file to signal to automated bots that they are prohibited from accessing LinkedIn servers, blocking automated attempts to scrape data, and barring such behavior through its User Agreement.[2]

When LinkedIn sent hiQ a cease-and-desist letter, hiQ filed a lawsuit seeking a declaratory judgment that it had access to LinkedIn's public data. LinkedIn's opposition to hiQ's motion for a preliminary injunction asserted that hiQ's actions violated copyright law and constituted trespass and misappropriation, but it primarily focused on its claim under the CFAA, which prohibits "access[ing] a computer without authorization or exceed[ing] authorized access."[3] The district court granted the preliminary injunction, enjoining LinkedIn from preventing hiQ from scraping its publicly available data. The Ninth Circuit affirmed, rejecting LinkedIn's CFAA claim because the profiles at issue were public, and "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."[4]

Van Buren and Remand

LinkedIn filed a cert petition, which was fully briefed.[5] On June 3, 2021, before the Supreme Court considered the petition, it issued its decision in *Van Buren v. United States*, which strictly limited the potential reach of CFAA claims. The Court held that "exceed[ing] authorized access" under the CFAA only prohibits unauthorized *access*, not unauthorized uses.[6] Although it did not explicitly say so, the Court's interpretation largely mirrored that of the Ninth Circuit in *hiQ* and earlier cases.[7]

LinkedIn filed an additional brief following *Van Buren*, requesting that the Court grant cert on the CFAA's definition of "without authorization," the prong of the CFAA under which the Ninth Circuit had rendered its decision.[8] However, in *Van Buren*, the Court had endorsed a "gates-up-or-down" approach for both prongs of the CFAA: "One either can or cannot access a computer system, and one either can or cannot access certain areas within the system."[9] The Supreme Court granted LinkedIn's cert petition the following week, but only to vacate the Ninth Circuit's decision and remand for further review.[10]

The Future of Scraping

As noted above, the CFAA has been one of the primary tools companies use to attack unauthorized scraping. While the Ninth Circuit had already limited the CFAA to only unauthorized access, some other circuits had not.[11] By limiting the scope of the CFAA, *Van Buren* weakened this defense against scrapers. *Van Buren* did not make the CFAA entirely obsolete, however, and it left unanswered the important question of whether only technological limitations qualify as "gates," or whether contractual limits, such as those in LinkedIn's User Agreement, would also qualify.[12]

It is likely that following *Van Buren*, those wishing to stymie scraping of their online data will increasingly need to rely on other causes of action, as the Ninth Circuit suggested in *hiQ*.[13] For example, claims have been successfully brought against scrapers for breach of contract,[14] circumvention of the Digital Millennium Copyright Act,[15] and copyright infringement,[16] among others. Companies wishing to prohibit scraping may need to consider whether to require a password to access some or all of the data so that it is clear when the "gates are down," as well as contemplate other anti-scraping causes of action as part of their litigation strategies.

---

1 Petition Granted, *LinkedIn Corp. v. hiQ Labs, Inc.*, 19-1116 (Sup. Ct. June 14, 2021).

2 *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 990-91 (9th Cir. 2019).

3 18 U.S.C. § 1030(a)(2) (2018).

4 *Id.* at 992, 995, 1003.

5 Petition for a Writ of Certiorari, *LinkedIn Corp. v. hiQ Labs, Inc.*, 19-1116 (Sup. Ct. Mar. 9, 2020).

6 *Van Buren v. United States*, Slip Opinion, No. 19-783, 20 (Sup. Ct. June 3, 2021).

7 *United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012) (en banc).

8 Petitioner's Supplemental Brief, *LinkedIn Corp. v. hiQ Labs, Inc.*, 19-1116 (Sup. Ct. June 7, 2020).

9 *Van Buren*, No, 19-783, at 14.

10 Petition Granted, *LinkedIn Corp. v. hiQ Labs, Inc.*, 19-1116 (Sup. Ct. June 14, 2021).

11 *See U.S. v. John*, 597 F.3d 263, 271 (5th Cir. 2010); *U.S. v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010); *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 421 (7th Cir. 2006); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 583 (1st Cir. 2001).

12 *Van Buren*, No, 19-783, at 13 n.8.

13 *hiQ*, 938 F.3d at 1004 ("[V]ictims of data scraping are not without resort, even if the CFAA does not apply: state law trespass to chattels claims may still be available. And other causes of action, such as copyright infringement, misappropriation, unjust enrichment, conversion, breach of contract, or breach of privacy, may also lie.").

14 *See, e.g., Ticketmaster L.L.C. v. RMG Techs., Inc.*, 507 F. Supp. 2d 1096, 1111-12 (C.D. Cal. 2007).

15 *See, e.g., Healthcare Advocates, Inc. v. Harding, Early, Follmer & Frailey*, 497 F. Supp. 2d 627, 642 (E.D. Pa. 2007).

16 *See, e.g., AP v. Meltwater News*, 931 F.Supp.2d 537, 561 (S.D.N.Y. 2013)

If you have questions concerning the contents of this issue, or would like more information about Weil's IP/Media practice group, please speak to your regular contact at Weil, or to the editors or practice group members listed below:

Editor:

Randi Singer (NY)	View Bio	randi.singer@weil.com	+1 212 310 8152

Contributing Authors:

Randi Singer (NY)	View Bio	randi.singer@weil.com	+1 212 310 8152
Michael Goodyear (NY)	View Bio	michael.goodyear@weil.com	+1 212 310 8213

© 2021 Weil, Gotshal & Manges LLP. All rights reserved. Quotation with attribution is permitted. This publication provides general information and should not be used or taken as legal advice for specific situations that depend on the evaluation of precise factual circumstances. The views expressed in these articles reflect those of the authors and not necessarily the views of Weil, Gotshal & Manges LLP. If you would like to add a colleague to our mailing list, please click here. If you need to change or remove your name from our mailing list, send an email to weil.alerts@weil.com.