Proskauer

# Supreme Court Vacates LinkedIn-HiQ Scraping Decision, Remands to Ninth Circuit for Another Look

**New Media and Technology Law Blog** on **June 16, 2021**

On June 14, 2021, in a closely-watched dispute involving the Computer Fraud and Abuse Act (CFAA), the Supreme Court granted LinkedIn Corp.'s ("LinkedIn") petition for certiorari filed in the *hiQ* web scraping case. It subsequently vacated the Ninth Circuit 2019 opinion and remanded the case to the Ninth Circuit for further consideration in light of the Supreme Court's decision from earlier this month in *Van Buren v. United States*, 593 U. S. ___ (June 3, 2021). (*LinkedIn Corp. v. hiQ Labs, Inc.*, No. 19-1116, 593 U.S. ___ (GVR Order June 14, 2021)).

In *Van Buren*, the Supreme Court reversed an Eleventh Circuit decision and adopted a narrow interpretation of "exceeds unauthorized access" under the CFAA, ruling that an individual "exceeds authorized access" when he or she accesses a computer with authorization but then obtains information located in particular areas of the computer – such as files, folders, or databases – that are off limits to him or her.

The LinkedIn-hiQ dispute involves a different part of the CFAA's "unauthorized access" section than the *Van Buren* case. The question in the *hiQ* dispute concerns the scope of CFAA liability to unwanted web scraping of publicly available social media profile data and whether once data analytics firm hiQ received a cease-and-desist letter from LinkedIn demanding it stop scraping public profiles, any further scraping of such data was "without authorization" within the meaning of the CFAA. In 2017 the lower court issued a preliminary injunction, expressing "serious doubt" as to whether LinkedIn's revocation of permission to access the public portions of its site rendered hiQ's access "without authorization" within the meaning of the CFAA. On appeal, in 2019 the Ninth Circuit affirmed, notably ruling that: "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." In 2020 LinkedIn filed a petition for a writ of certiorari asking the Supreme Court to overturn the Ninth Circuit's ruling. And now, in the wake of *Van Buren*, the Supreme Court has vacated the appeals court ruling and sent the case back to the Ninth Circuit for further consideration.

So what's next? Some thoughts:

**Direct effect of *Van Buren***

The *hiQ* and *Van Buren* cases involve different parts of the CFAA's "unauthorized access" provision. So, on remand, while the *Van Buren* holding on "exceeds authorized access" under the CFAA will lend some clarity to how the Ninth Circuit might interpret the CFAA generally and how to view authorization generally, it will be up to the appeals court to determine whether hiQ's continued scraping following LinkedIn's blocking efforts constituted "unauthorized access" (an undefined term under the CFAA).

Notably, *Van Buren* espoused a "gates-up-and-down" approach to CFAA liability:

> "Van Buren's account of subsection (a)(2) 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."

Thus, the question in *hiQ* will likely hinge on whether technical measures to block access to LinkedIn's site followed by a formal revocation of access truly lowers the access gate (for purposes of CFAA liability) or whether the gate for public website content is always up and no CFAA liability may arise for such access to publicly available website data.

**Authorization issue much different in *Van Buren***

Putting aside the Court's examination of the CFAA "exceeds authorized access" issue in *Van Buren*, the issue of authorization in the *Van Buren* case was clear-cut (i.e., the former police officer had authorized access to the license plate database at issue, but accessed it for an improper purpose). However, in the *hiQ* scraping context, the CFAA "without authorization" issue is more nuanced. The appeals court will be asked again to decide whether the CFAA's "without authorization" provision is limited to computer information for which access permission, such as password authentication, is generally required.

**Footnote 8 back in the spotlight**

When the Supreme Court in *Van Buren* discussed the concept of a "gates-up-or-down" approach to understanding the CFAA's "without authorization" and "exceeds authorized access" clauses, it wrote the following: "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." There, it dropped what promises to be one of the most cited footnotes in subsequent decisions by lower courts, Footnote 8, that leaves certain questions – relevant to the LinkedIn case – for another day. In Footnote 8, the Court stated: "For present purposes, we need not address whether this inquiry turns only on technological (or "code-based") limitations on access, or instead also looks to limits contained in contracts or policies." Having declined to decide whether authorized access turns on only code-based restrictions, the Court placed this issue back in the Ninth Circuit's lap with the *hiQ* remand.

In its Supplemental Brief filed with the Supreme Court following the *Van Buren* decision, LinkedIn brought up this very issue, stating the uncertainty surrounding whether measures undertaken by website operators are effective "gates" blocking authorized access or not:

> "Websites employ myriad strategies that might or might not qualify as 'gates,' from code-based measures such as password requirements and LinkedIn's technical blocking measures, to express communications such as cease-and-desist letters, to the contracts and policies mentioned in Van Buren."

LinkedIn argued that it had placed "gates" around its servers by using code-based technical measures to block hiQ's bots and scraping activities and also by sending a cease-and-desist letter revoking access. However, with the Supreme Court declining to take up LinkedIn's appeal on the merits, it will be left to the Ninth Circuit to presumably parse Footnote 8's ambiguity to decide what measures raise or lower the "gates" of authorization.

**Final thoughts**

With *Van Buren* having taken a narrow approach to the CFAA's "exceeds authorized access" provision, it would not be surprising if the Ninth Circuit reaches the same narrow conclusion as its 2019 ruling regarding access "without authorization." Regardless of the outcome, the appeals court's reconsideration of the case may offer some clarity as to whether only code-based measures can lower the authorization gates or whether other actions may achieve the same revocation of access in the context of public website content. Moreover, since the *hiQ* case involves publicly available website data, it may be that this issue carries the day once again in the court's renewed preliminary injunction analysis, both from a legal and public policy/balancing of the equities perspective. Recall, such issues were vital in its original reasoning on these issues:

> "Public LinkedIn profiles, available to anyone with an Internet connection, fall into the first category [information for which access is open to the general public and permission is not required]."
>
> "We agree with the district court that giving companies like LinkedIn free rein to decide, on any basis, who can collect and use data—data that the companies do not own, that they otherwise make publicly available to viewers, and that the companies themselves collect and use—risks the possible creation of information monopolies that would disserve the public interest."

Still, it remains to be seen how the Ninth Circuit will ultimately rule when it revisits this case, particularly given the multiple incidents of unwanted scraping of social media content on a massive scale that have occurred in the past year, perhaps bolstering LinkedIn's policy argument on the need to protect user privacy. Needless to say, we will be watching closely.

View Original

**Related Professionals**

- **Jeffrey D. Neuburger**