The Ninth Circuit Rejects (Again) LinkedIn's Attempt to Prevent Web-Scraping of Its Publicly Available Member Profiles under the Computer Fraud & Abuse Act (CFAA)

May 19, 2022 Lee Johnston

PRACTICES Media Entertainment and Sports, Anti-SLAPP and First Amendment Rights

On April 18, 2022, the Ninth Circuit, in *hiQ Labs v. LinkedIn Corporation*, 41 F. 4th 1180 (9th Cir. 2022), upheld (again) a 2018 injunction which enjoined LinkedIn from preventing its small start-up competitor, hiQ, from accessing and scraping data from LinkedIn members' public profiles. The Ninth Circuit's ruling has likely dealt the final death blow to website owners' attempts to use the CFAA as a means to combat web-scraping activity on their public-facing web pages.

To better understand the Ninth Circuit's most recent decision, it is useful to take a look back at this long-running David versus Goliath battle.

The Ninth Circuit's 2019 Decision ("*LinkedIn I*").

As previously reported in our Fall 2019 newsletter, the Ninth Circuit's 2019 opinion in *hiQ* handed web- scrapers an important win. In its 2019 decision, the Ninth Circuit held that the CFAA's prohibition against "unauthorized access" to a "protected computer" did not shield LinkedIn from HiQ's tortious interference with contract and unfair competition claims, which hiQ had brought to enjoin LinkedIn's use of anti-bot technology that prevented hiQ from scraping LinkedIn members' data from their public-facing web profiles. In upholding the trial court's injunction, the Ninth Circuit found that the CFAA's "without authorization" element could not be met if no authorization was required in the first place, as with publicly facing, non-password protected web pages. Media companies, which saw LinkedIn's attempt to selectively prohibit access to publicly available information as a threat to the First Amendment's core values, lauded the Ninth Circuit's 2019 decision.

The Supreme Court Vacates and Remands Back to the Ninth Circuit -- *Van Burren* and the "Gates Up/Gates Down" Application of the CFAA's "Exceeds Authorized Access" Element.

As often happens when data privacy and public access interests collide, the battle was not over. LinkedIn sought Supreme Court review, arguing that the Ninth Circuit's decision trampled on its right to revoke access to bad actors who, like hiQ, had been specifically advised that their refusal to abide by LinkedIn's "Terms of Use" policy (which prohibited web-scraping) would result in termination of privileges to LinkedIn's web site. As discussed in our Spring 2021 newsletter, the Supreme Court appeared to view LinkedIn's position favorably by granting LinkedIn's certiorari petition, vacating the Ninth Circuit's *LinkedIn I* decision, and remanding the case back to the Ninth Circuit. In its June 14, 2021, remand order, the Supreme Court specifically directed the Ninth Circuit to re-assess its *LinkedIn I* opinion in light of the Supreme Court's decision issued ten days earlier in *Van Buren v. United States*.[1]

In *Van Buren*, Justice Amy Coney Barrett wrote for a 6-3 majority that the CFAA contemplates a "gates up or down" approach to determining liability under the CFAA. In the Court's view, one only

"exceeds authorized access" when accessing a computer with authorization but then obtaining information located in particular areas of the computer – such as files, folders, or databases – that are off-limits (*i.e.*, where the gates are "down"). In holding that the accessing of authorized areas of a computer for improper purposes no longer creates a CFAA violation, the Court expressed concerns that a more expansive reading of the CFAA would create criminal liability for millions of otherwise law-abiding citizens. Justice Barrett observed that most workplaces have policies limiting computer use to business purposes; as a result, under a more expansive definition of "exceeds authorized access," anyone who agrees to such a policy and then sends a personal email from a work computer would commit a felony violation of the CFAA. Similarly, the Court noted that many websites require users to agree to detailed terms of service as a condition of access, and that the expansive reading would "criminalize everything from embellishing an online-dating profile to using a pseudonym on [social media]."

The Ninth Circuit Applies *Van Buren* and Re-Affirms hiQ's Injunction (*LinkedIn II*).

On remand, the Ninth Circuit noted that the "pivotal CFAA question" was "whether once hiQ received LinkedIn's cease-and-desist letter, any further scraping and use of LinkedIn's data was 'without authorization' within the meaning of the CFAA and thus a violation of the statute." In answering this question in the negative – and finding that the CFAA did not apply to hiQ's data scraping -- the Ninth Circuit took an approach similar to the 2019 *LinkedIn I* decision, drawing support for its holding from the Supreme Court's *Van Buren* decision.

First, the court reasoned that the phrase "'without authorization' suggests a baseline in which access is not generally available and so permission is ordinarily required." On the flip side, the court found that "where the default is free access without authorization, in ordinary parlance one would characterize selective denial of access as a ban, not as a lack of 'authorization.'" With this framework established, the Ninth Circuit returned to its *LinkedIn I* conclusion that the CFAA contemplates the existence of three kinds of computer systems that can be accessed: (1) computers for which access is open to the general public and permission is not required; (2) computers for which authorization is required and has been given; and (3) computers for which authorization is required but has not been given. According to the Ninth Circuit, the publicly available LinkedIn member web pages fell into the first category, and thus, the CFAA's prohibition against access without authorization was "inapt" and simply did not cover hiQ's conduct.

To bolster its conclusion, the court pointed to the Supreme Court's *Van Buren*'s "gates up/gates down" framework. According to the Ninth Circuit, the Court's "gates up/gates down" inquiry applied to the latter two categories of computer systems; the first category of computer systems, hosting publicly available webpages like LinkedIn's member public pages has no gates to lift or lower in the first place.

Where We Go from Here

Van Buren and *LinkedIn II* will likely eliminate CFAA claims based on a violation of a terms of use policy. Indeed, it is doubtful that a CFAA claim will stand unless a defendant circumvents technological barriers which are intended to serve as a "gates down" prohibition on access. Nonetheless, as district court decisions after *Van Buren* have demonstrated,[2] companies seeking to prevent, or at least hinder, web scraping on their websites should continue to evaluate and update their terms of service agreements and maintain records documenting users' consents to these terms in order to preserve their ability to obtain injunctive relief based on contract and trespass-to-chattel-based claims. In addition, businesses should implement technological barriers, such as password implementation and network segmentation, to prevent access to sensitive data.

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

[2] *See, e.g., Southwest Airlines Co. v. Kiwi.com, Inc*. Civil Action No. 21-00098 (N.D. Tex. Sept. 30, 2021) (enjoining competitor's access to Southwest Airlines' flight fare data, finding that Southwest was likely to succeed on its contract claim based on its Terms of Service policy, which the competitor consented to in order to access Southwest's data).