The Computer & Internet Lawyer

Volume 39 ▲ Number 2 ▲ February 2022

Ronald L. Johnston, Arnold & Porter, Editor-in-Chief

The Shifting Legal Landscape Surrounding Web Scraping

By Lee F. Johnston

The landmark decision by the U.S. Court of Appeals for the Ninth Circuit decision in *hiQ v. LinkedIn* provided an important win for web scrapers.[1]

In *hiQ*, the Ninth Circuit upheld the trial court's injunction enjoining LinkedIn from using technological measures to prevent hiQ from scraping data from the public profiles of LinkedIn members. To reach this result, the Ninth Circuit found that the prohibition in the Computer Fraud & Abuse Act ("CFAA") against "unauthorized access" to "protected computers" did not apply to web scraping of data appearing on publicly available web pages. According to the Ninth Circuit, LinkedIn's attempts to "revoke" hiQ's authorization to access LinkedIn's members' public profiles – through cease-and-desist letters and technological anti-scraping means – could not establish CFAA liability, since profiles which were freely available and accessible to the public needed no "authorization" in the first place.

Lee F. Johnston, a partner in the Denver office of Haynes and Boone, LLP, is a trial lawyer whose national trial practice includes patent, copyright, trademark and trade secret litigation. Mr. Johnston may be contacted at *lee.johnston@haynesboone.com*.

LinkedIn filed its Petition for Writ of Certiorari at the U.S. Supreme Court on March 6, 2020. On June 3, 2021, with LinkedIn's petition still pending, the Supreme Court issued its opinion in *Van Buren v. United States*,[2] addressing the scope of the CFAA in the context of a criminal conviction under the CFAA's prohibition against conduct involving the access of a protected computer which "exceeded authorization."

The *Van Buren* Decision – No CFAA Liability for Accessing for Improper Purpose

Former Georgia police Sergeant Nathan Van Buren was prosecuted for accessing a law enforcement database from his cruiser to look up the owner and address information for a particular license plate, which Van Buren did so in exchange for money. Van Buren used his valid credentials to access the database, but in doing so, he violated a department policy prohibiting use of the database for purposes other than police business. Van Buren was charged with and convicted of a felony violation of the CFAA and sentenced to 18 months in prison. The Eleventh Circuit upheld his conviction, finding that Officer Van Buren had exceeded his "authorized

access" when he accessed the license plate database for an "inappropriate reason."[3]

In the majority opinion for a 6-3 decision overturning Van Buren's conviction, Justice Amy Coney Barrett wrote that the CFAA contemplates a "gates up or down" approach to determining liability under the CFAA. In the Court's view,an individual 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 to him. Since Van Buren was authorized to access the license plate database, he had not "exceeded" his authorization under the CFAA.

In holding that the accessing of authorized areas of a computer for improper purposes no longer creates a CFAA violation, the Court expressed concern 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, and under a more expansive definition of "exceeds authorized access," anyone who agreed to such a policy and then sent a personal email would have committed 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 an expansive reading would "criminalize everything from embellishing an online-dating profile to using a pseudonym on [social media]."[4]

Web Scraping In The Aftermath of *Van Buren* – Remaining CFAA Questions and Pursuit of Non-CFAA Claims

Although the Supreme Court did clarify the CFAA in *Van Buren*, some ambiguity remains. The Court expressly declined to resolve the issue of whether the "gates up-or-down" access depends on whether access is prohibited by limitations created by technological barriers, such as passwords, or by contractual limitations, such as employment agreements.

Unfortunately, the Court declined to address this issue directly when it had the opportunity to do so in the pending *hiQ v. LinkedIn* case. Instead, the Court issued a cursory opinion vacating and remanding the Ninth Circuit's judgment for further consideration in light of *Van Buren*.[5] Although we do not know for sure, the Court likely interpreted LinkedIn's user agreement's prohibition against web-scraping bots as a limitation on use, instead of a limitation on access. Answers to these questions must now await the Ninth Circuit's decision on remand.

In view of these remaining questions, website owners have successfully pressed non-CFAA claims, most notably breach of contract claims, as a vehicle to prevent web-scraping activities. On September 30, 2021, the U.S. District Court for the Northern District of Texas granted Southwest Airline Co. a preliminary injunction preventing online travel site Kiwi.com from, among other things, scraping fare data from Southwest's website and committing other acts that violate Southwest's terms of service.[6] The Texas court rejected Kiwi's arguments that it did not agree to Southwest's terms, finding that Kiwi had knowledge of and assented to the terms in multiple ways, including by agreeing to the terms when purchasing Southwest's tickets on Southwest's website. In all, the court found the existence of a valid contract and Kiwi's likely breach of its terms, which prohibit scraping of Southwest's flight data and selling Southwest's flights without authorization.

One of the more interesting aspects of the court's opinion is how the court dealt with the Ninth Circuit's 2019 *hiQ* decision. While not pressed in its motion for preliminary injunction motion, Southwest had included a CFAA claim in its second amended complaint. One of Kiwi's main arguments against the injunction was that since it was scraping publicly available data, the *hiQ* ruling meant that Southwest could not establish a likelihood of success on its contract claim. In deflecting that argument, the court pointed out that the Ninth Circuit itself had left open the possibility of other claims – such as the contract claim which Southwest pursued in its PI motion – as providing the basis for injunctive relief.

Takeaways and Recommendations

The Supreme Court's *Van Buren* decision likely spells the death knell of 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 the ruling in *Southwest Airlines v. Kiwi* demonstrates, 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 successfully seek injunctive relief based on contract-based claims.

In addition, businesses should implement technological barriers to prevent access to their sensitive data. Technological barriers include password implementation, which restricts who can access sensitive data, and network segmentation, which divides a network into subnetworks and restricts who can access certain sensitive data.

Notes

1. 938 F.3d 985 (9th Cir. 2019).
2. *Van Buren v. United States*, 141 S.Ct. 1648 (2021).
3. 940 F3d. 1192, 1208 (11th Cir. 2019).
4. 141 S.Ct. at 1661.
5. 121 S.Ct. 2752 (2021).
6. *See Southwest Airlines Co. v. Kiwi.com, Inc.* No. 3:21-cv-00098-E (N.D. Tex. Sept. 30, 2021).