Tech & Telecom Law

Data Scraping in a Post-*hiQ* World

By Jason Russell and Matthew Tako

May 17, 2022, 4:00 AM

A recent Ninth Circuit ruling, combined with a U.S. Supreme Court case involving unauthorized access under the Computer Fraud and Abuse Act, suggests that courts will not view data scraping of public information as a violation of the CFAA. Skadden attorneys Jason Russell and Matthew Tako offer options for companies to protect their data, including updating terms and conditions prohibiting scraping and copyrighting the material.

The U.S. Court of Appeals for the Ninth Circuit last month upheld an order denying LinkedIn from preventing hiQ Labs from scraping the professional networking site's job search data.

The case was on remand from the U.S. Supreme Court in light of the high court's 2021 decision in *Van Buren v. United States*, which limited the reach of the decades-old Computer Fraud and Abuse Act (CFAA).

At the core of the Ninth Circuit's analysis in *hiQ Labs Inc. v. LinkedIn Corp.* was whether hiQ's scraping of publicly accessible data from LinkedIn profiles, even after LinkedIn sent a cease-and-desist letter, constituted unauthorized access of a computer in violation of the CFAA. According to the court, hiQ raised a serious question as to whether the CFAA's "without authorization" language applies to public information which is freely available to any internet user, such that a preliminary injunction was warranted.

The case has now been remanded to the district court for further proceedings.

In light of the *hiQ* ruling, companies should rethink their approach for countering scraping activity. A cease-and-desist letter, on its own or together with IP address blocking (preventing access), will not suffice to implicate the CFAA, at least in the Ninth Circuit.

While *hiQ* creates a significant uphill battle for stating a valid CFAA claim for scraping information from an otherwise publicly available site, it does not foreclose other potential causes of action which can still deter or prevent scraping.

Two examples of such claims include copyright infringement and trespass.

Copyright Infringement

As the court noted in *hiQ,* copyright infringement remains a valid claim for when a scraper is taking and repurposing copyrighted information. In *Associated Press v. Meltwater U.S. Holdings Inc.*, a federal district court in New York found that scraping copyrighted news articles and then repacking them in a subscription newsletter did not constitute fair use and was instead copyright infringement.

In *Meltwater*, the scraper tried to classify itself as a search engine in an effort to circumvent copyright laws. But the court rejected the search engine classification, noting that the scraper was "an expensive subscription service" that was "neither designed nor operated to improve access to the complete, linked news story," nor was it a "publicly available tool to improve access to content across the internet."

Trespass

The *hiQ* court also noted that a scraper acting in violation of a cease-and-desist letter may still give rise to a common law tort claim for trespass. A plaintiff's lack of consent is critical to any trespass claim. As such, if a company operates a publicly accessible website, it should lay a clear marker that any potential scraping activity is not welcome, both in its terms of service as well as via a cease-and-desist letter. Several courts have weighed this issue, to mixed results.

For example, in *eBay Inc. v. Bidder's Edge Inc.*, a federal district court found a likelihood of success on a trespass claim was established because even though a site was publicly accessible, its servers were private property and scraping activity exceeded the scope of consent.

And in *Register.com Inc. v. Verio Inc.*, the Second Circuit held that scraping constituted trespass because it could, even if it had not yet, cause physical harm, to a company's servers.

But other courts have found no trespass occurred when harm to the company's servers or computer operations did not occur.

In both *Ticketmaster Corp. v. Tickets.Com Inc.* and *Intel Corp. v. Hamidi*, mere scraping, without more, such as "actual or threatened injury" to property through damaging or interfering with a company's computer systems, did not rise to the level of trespass.

Other Potential Claims

In addition to copyright infringement and trespass, companies targeted by scrapers will want to consider other, similar claims which exist in their jurisdictions. Such claims may include state-specific hacking laws, like California Penal Code Section 502, unjust enrichment, or conversion.

Key Takeaways

The recent *Van Buren* and *hiQ* opinions suggest that courts will not view scraping data from a website which an ordinary user is freely able to visit as "unauthorized access" that violates the CFAA. If a company is looking to counter potential scraping activity, it should consider several options.

First, even if a cease-and-desist letter on its own may not withdraw access under the CFAA, one should still be sent to any scrapers to assist in establishing common law claims such as trespass.

Second, website terms and conditions should similarly state that scraping activity is not permitted.

Third, companies should monitor what impact scraping may have on the functioning of their servers, such as increased website load times for other users or costs associated with establishing authenticating systems to counter scraping activity. This will help establish damages where required.

Fourth, if applicable, companies should indicate that the information on their sites are copyrighted.

Finally, companies should consider what information is freely available versus what information is kept behind a user login credential portal. If the user terms include an anti-scraping provision, companies can look to exercise those terms and invalidate the credentials of any scraper.

Companies should then follow up with written notification that the offender is banned under any alternate login credentials which may be created or used to continue the scraping activity. Creating additional accounts to continue such activity after previous credentials were revoked may ultimately be seen as a violation of the CFAA, as well as numerous other state law tort claims.

This article does not necessarily reflect the opinion of The Bureau of National Affairs, Inc., the publisher of Bloomberg Law and Bloomberg Tax, or its owners.

Write for Us: Author Guidelines

Author Information

Jason Russell is head of Skadden's Los Angeles office, representing a wide variety of clients in commercial litigation disputes in federal and state courts throughout the country as well as in international forums.

Matthew Tako is a litigation associate in Skadden's Los Angeles office. His practice focuses on both civil and criminal matters, with his representations including financial services firms, technology companies, restaurants, automakers and individuals in connection with litigation and investigations by both federal and state agencies.