GIBSON DUNN

September 16, 2019

NINTH CIRCUIT ISSUES DECISION IN CLOSELY WATCHED DATA SCRAPING CASE

To Our Clients and Friends:

On September 9, 2019, the Ninth Circuit issued its long-anticipated decision in *hiQ v. LinkedIn*, one of the most closely watched data scraping cases in years. Affirming the district court's decision, the Ninth Circuit held that data analytics company hiQ was entitled to a preliminary injunction forbidding LinkedIn from denying hiQ access to publicly available LinkedIn member profiles.

Background

Many companies harvest or "scrape" electronic data from third parties—sometimes with that third party's permission, sometimes without. In some cases, data analytics companies like hiQ scrape data, aggregate it, apply their own algorithm, and sell the resulting data analytics products and services. In other cases, companies may scrape data for internal research purposes.

hiQ's case against LinkedIn attracted significant interest from data hosting platforms, data analytics companies, and other companies that engage in data scraping, as well as from public interest organizations that were divided over the issue, with the Electronic Privacy Information Center warning of the privacy risks associated with data scraping, while the Electronic Frontier Foundation and other entities emphasized the need for open access to information online.

The Issue in *hiQ v. LinkedIn*

LinkedIn is a professional networking website with over 500 million members, on which users post resumes and job listings and build connections with other members. LinkedIn members retain ownership of the information they submit, which they license non-exclusively to LinkedIn. Members can choose whether to make their LinkedIn profiles visible only to direct connections, to certain LinkedIn members, to all LinkedIn members, or—as relevant here—to the general public.

hiQ Labs is a data analytics company that uses automated bots to scrape information from public LinkedIn profiles, and then aggregates that data to create "people analytics" tools that it sells to business clients. In May 2017, LinkedIn sent hiQ a cease-and-desist letter, asserting that hiQ violated LinkedIn's User Agreement, demanding that hiQ stop accessing and copying user data from LinkedIn, and warning hiQ that continued activity would violate state and federal law, including the Computer Fraud and Abuse Act ("CFAA"), the Digital Millennium Copyright Act ("DMCA"), and the California common law of trespass. Shortly after, hiQ filed suit, seeking injunctive and declaratory relief in order to continue scraping data from LinkedIn's public pages. In August 2017, the district court granted hiQ's motion for a preliminary injunction and ordered LinkedIn to refrain from enacting any legal or technical barriers to hiQ's access to public profiles. The Ninth Circuit heard oral argument in March 2018.

The Ninth Circuit's Opinion

In an opinion authored by Judge Marsha S. Berzon, the Ninth Circuit affirmed the district court's grant of a preliminary injunction.

First, the Ninth Circuit found that hiQ had demonstrated a likelihood of irreparable harm absent a preliminary injunction. Crediting the district court's determination that hiQ's entire business depends on access to public LinkedIn profiles, the Ninth Circuit found that the record supported hiQ's assertions that it would be forced to breach existing contracts, forgo prospective deals, lay off most of its employees, and shutter its business absent a preliminary injunction.

Second, the Ninth Circuit upheld the district court's determination that the balance of hardships tips in favor of hiQ, pointing out that LinkedIn has no protected property interest in the data contributed by its users, who retain ownership over their profiles, and that LinkedIn users who choose to make their profiles public have little expectation of privacy with respect to the information they post publicly.

Third, the Ninth Circuit held that, under the sliding-scale approach to the preliminary injunction factors, because the balance of hardships tipped decidedly in hiQ's favor, hiQ satisfied the likelihood-of-success prong by raising serious questions going to the merits. The Ninth Circuit agreed with the district court that hiQ had shown a likelihood of success on its tortious interference with contract claim, pointing out that LinkedIn knew hiQ scraped data from its servers for hiQ's own products and services, and that LinkedIn's competitive business interests were insufficient to justify its interference with hiQ's existing contracts.

The Ninth Circuit rejected LinkedIn's affirmative defense that hiQ had accessed LinkedIn data "without authorization" under the CFAA, 18 U.S.C. § 1030, and that the CFAA preempted hiQ's state law claims. Authorization, the panel wrote, "is an affirmative notion, indicating that access is restricted to those specially recognized or admitted": The wording of the statutory phrase "'[a]ccess[] . . . without authorization,' 18 U.S.C. § 1030(a)(2), suggests a baseline in which access is not generally available and so permission is ordinarily required." That interpretation, Judge Berzon noted, is confirmed by the legislative history of the CFAA, which was enacted to prevent intentional computer hacking—an act "analogous to that of 'breaking and entering.'" "Public LinkedIn profiles, available to anyone with an Internet connection," the Court explained, therefore do not constitute information for which authorization or access permission is generally required. Further, the Ninth Circuit cautioned that the rule of lenity favors a narrow interpretation of the "without authorization" provision, as Section 1030 is primarily a criminal statute and statutes must be interpreted consistently in the criminal and civil contexts.

Finally, the Ninth Circuit found that, on balance, the public interest favors granting the preliminary injunction. The Ninth Circuit observed that, although LinkedIn had an obvious interest in blocking abusive users and thwarting attacks on its servers, the injunction does not prevent it from employing anti-bot measures to combat such abuses. And permitting companies like LinkedIn that collect large amounts of data "to decide, on any basis, who can collect and use" user data posted publicly on their platforms "risks the possible creation of information monopolies that would disserve the public interest."

What To Expect

The Ninth Circuit's opinion—although framed narrowly as deferring to the district court's determinations on the preliminary injunction record in this case—is likely to be relied upon by companies seeking to scrape publicly available data from public websites.

The contours of Section 1030 liability have been the subject of competing interpretations in different Circuits. The First, Fifth, Seventh, and Eleventh Circuits have adopted a broad view of the CFAA, extending Section 1030 liability even to misuse or misappropriation of information lawfully accessed, as when a corporate employee with valid login credentials provides files to a competitor, *see, e.g.*, *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010); *United States v. John*, 597 F.3d 263, 271 (5th Cir. 2010); *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420–21 (7th Cir. 2006); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 581–84 (1st Cir. 2001), and permitting civil CFAA claims to proceed based on violations of a website's terms of service, *Sw. Airlines Co. v. Farechase, Inc.*, 318 F. Supp. 2d 435, 439–40 (N.D. Tex. 2004). By contrast, the Second, Fourth, and Ninth Circuits have adopted a narrow view, interpreting the CFAA as a restriction on unauthorized access rather than on "mere use of a computer" (including use in violation of a website's terms of service), and thus limiting Section 1030 liability to those who, through disingenuous means, gain *access* to data in a manner analogous to "breaking and entering." H.R. Rep. No. 98–894, at 3706 (1984); *see, e.g.*, *United States v. Valle*, 807 F.3d 508, 523–28 (2d Cir. 2015); *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 205–06 (4th Cir. 2012); *United States v. Nosal (Nosal I)*, 676 F.3d 854, 857–63 (9th Cir. 2012) (en banc). The decision in *hiQ v. LinkedIn* marks a long-anticipated addition to that landscape, reaffirming the Ninth Circuit's narrow approach while providing additional clarity as to the scope of Section 1030's "without authorization" provision.

Companies should not be too quick to view the Ninth Circuit's opinion as an invitation or green light to scrape, however. The Ninth Circuit was careful to point out that "victims of data scraping are not without resort" and, in particular, that accessing and scraping data without the website owner's consent may give rise to a common law tort claim for trespass to chattels. Going forward, we can expect that companies seeking to prevent data scraping will rely less on the CFAA and more on state law claims such as trespass to chattels. In addition, the Ninth Circuit's opinion "is premised on a distinction between information presumptively accessible to the general public and information for which authorization is generally required." Companies seeking to prevent scraping may attempt to demarcate data as non-public by requiring authorization or authentication measures or otherwise restricting access.

The following Gibson Dunn lawyers prepared this client update: Alexander Southwell, Matthew Benjamin, Alexandra Perloff-Giles and Erica Sollazzo Payne.

Gibson Dunn's lawyers are available to assist with any questions you may have regarding these issues. For further information, please contact the Gibson Dunn lawyer with whom you usually work or any of the following leaders and members of the firm's Privacy, Cybersecurity and Consumer Protection practice group:

United States

Alexander H. Southwell - Co-Chair, PCCP Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
M. Sean Royall - Dallas (+1 214-698-3256, sroyall@gibsondunn.com)
Debra Wong Yang - Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)
Olivia Adendorff - Dallas (+1 214-698-3159, oadendorff@gibsondunn.com)
Matthew Benjamin - New York (+1 212-351-4079, mbenjamin@gibsondunn.com)
Ryan T. Bergsieker - Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
Richard H. Cunningham - Denver (+1 303-298-5752, rhcunningham@gibsondunn.com)
Howard S. Hogan - Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)
Joshua A. Jessen - Orange County/Palo Alto (+1 949-451-4114/+1 650-849-5375, jjessen@gibsondunn.com)
Kristin A. Linsley - San Francisco (+1 415-393-8395, klinsley@gibsondunn.com)
Karl G. Nelson - Dallas (+1 214-698-3203, knelson@gibsondunn.com)
Eric D. Vandevelde - Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Benjamin B. Wagner - Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)
Michael Li-Ming Wong - San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)

Europe

Ahmed Baladi - Co-Chair, PCCP Practice, Paris (+33 (0)1 56 43 13 00, abaladi@gibsondunn.com)
James A. Cox - London (+44 (0)207071 4250, jacox@gibsondunn.com)
Patrick Doris - London (+44 (0)20 7071 4276, pdoris@gibsondunn.com)
Penny Madden - London (+44 (0)20 7071 4226, pmadden@gibsondunn.com)
Jean-Philippe Robé - Paris (+33 (0)1 56 43 13 00, jrobe@gibsondunn.com)
Michael Walther - Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Kai Gesing - Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Sarah Wazen - London (+44 (0)20 7071 4203, swazen@gibsondunn.com)
Vera Lukic - Paris (+33 (0)1 56 43 13 00, vlukic@gibsondunn.com)
Alejandro Guerrero - Brussels (+32 2 554 7218, aguerrero@gibsondunn.com)

Asia

Kelly Austin - Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)
Jai S. Pathak - Singapore (+65 6507 3683, jpathak@gibsondunn.com)