haynesboone

MEDIA, ENTERTAINMENT AND FIRST AMENDMENT NEWSLETTER

OCTOBER 2019

Lee Johnston

The Ninth Circuit Rejects LinkedIn’s Efforts to Block Web-Scraping of Member Public Profiles

Lee Johnston

Social media companies (“SMC’s”) are constantly working to leverage data they gather from customers to develop new, innovative products and effective advertising strategies to market those products. At the same time, SMC’s face threats from competitors seeking to harvest and exploit the publicly-available customer data hosted on SMC servers. On the technology side, SMC’s employ increasingly sophisticated artificial intelligence (AI)-based software to prevent automated bots and web crawlers from accessing and scraping customer data from SMC websites. And, under the auspices of enforcing their own proprietary rights and their customers’ privacy rights, SMC’s have asserted a variety of legal claims – ranging from common law trespass and breach of contract theories to federal copyright and Computer Fraud and Abuse Action (CFAA) claims -- in an effort to shut down, or at least deter, their competitors’ efforts to access and “scrape” SMC customer data.

As judges have gained a better understanding of the technology and legal issues in these cases, the viability of some of these claims has been circumscribed.[1] Nevertheless, SMC’s have largely been on the offensive in this battle, primarily due to their ability to outspend their competitors, which are often start-ups lacking the resources for extended legal battles. The Ninth Circuit’s September 9, 2019 decision in *hiQ Labs, Inc. v. LinkedIn Corporation*,[2] however, suggests a more favorable future for web scraping in general, and specifically highlights the effectiveness of smaller competitors’ strategy of “taking the battle” to larger SMCs rather than waiting to be sued.

HiQ Labs v. LinkedIn Corporation

In *hiQ* Labs, the Ninth Circuit affirmed the trial court’s preliminary injunction barring LinkedIn from blocking or otherwise hindering hiQ’s ability to “scrape” LinkedIn users’ public profiles. The underlying dispute in *hiQ* Labs centered on hiQ’s data analytics business model, which depends exclusively on its ability to scrape LinkedIn’s users’ public profile information. Using automated bots to harvest LinkedIn users' name, job title, work history and skills, hiQ applies a proprietary algorithm to this data to yield "people analytics," which it then sells to business clients to allow them to identify employees at the greatest risk of being recruited away, as well as to identify skill gaps in an employer's workforce.

LinkedIn took issue with hiQ's activities, especially because LinkedIn itself sought to develop and market its own skill-based predictive analytics product (Talent Insights) based on users' profiles. In May of 2017, therefore, LinkedIn sent hiQ a cease-and-desist letter, asserting that hiQ had violated LinkedIn's terms of use agreement, and that any future access of LinkedIn data would subject hiQ to liability under the CFAA, the Digital Millennium Copyright Act ("DMCA"), California Penal Code § 502(c) and the California common law of trespass.

Rather than taking a defensive posture, hiQ went on the offensive and filed a pre-emptive lawsuit seeking a declaration that it was legally entitled to scrape LinkedIn user profiles and that LinkedIn could not lawfully invoke the federal and state laws identified in its cease-and-desist letter. HiQ also went a step further, and sought an injunction prohibiting LinkedIn from erecting technological barriers to hiQ's automated bots. By doing so, hiQ effectively pivoted the Court's analysis, and instead of being seen as an Internet parasite, hiQ was able to successfully argue that it was the victim of LinkedIn's heavy-handed, anti-competitive tactics.[3] And, by posturing the case as one requiring immediate injunctive relief, hiQ highlighted its strongest argument – that LinkedIn's actions would destroy hiQ's business – and reduced its burden of proof on establishing the likelihood of success on the merits of its legal claims.[4]

HiQ's high-risk/high return legal strategy paid off, primarily due to (1) LinkedIn's inability to argue plausibly that its users' privacy interests were harmed by hiQ's conduct and (2) the Court's concern that a finding of liability under the CFAA would expand the statute's reach beyond what Congress intended. First, as to privacy concerns, both the trial court and Ninth Circuit found it significant that LinkedIn had no proprietary interest in the factual information contained in its users' online profiles. LinkedIn users, not LinkedIn, "owned" this factual data, and voluntarily chose to make their profiles available to the public. Indeed, LinkedIn's own privacy policy stated that "any information you put on your profile and any content you post on LinkedIn may be seen by others," and warned users not to "post or add personal data to your profile that you would not want to be public."[5] Moreover, LinkedIn's professed privacy concerns were undermined by the fact that LinkedIn allowed other third-parties to access user data without its members' knowledge or consent.

The trial court and the Ninth Circuit also expressed serious concerns about LinkedIn's CFAA argument that hiQ's violation of the LinkedIn website terms of use provisions and disregard of LinkedIn's subsequent cease-and-desist letter constituted violations of the CFAA's prohibition against computer access "without authorization." As the trial court noted, LinkedIn's interpretation of the CFAA would permit a website owner to revoke the "authorization" of any person at any time, for any reason, and then pursue civil and criminal penalties against that person for merely *viewing* the website – an outcome which the trial court characterized as "effectuating the digital equivalence of Medusa."[6] According to the trial court, allowing a private entity to effectively criminalize access to publicly viewable information, without any consideration of the website owner's reasons for denying access or an individual's possible justification for ignoring the website owner's denial of access, would be "particularly pernicious" to healthy competition and the public's right to information.[7]

The Ninth Circuit agreed that the CFAA's prohibition against accessing a protected "without authorization" must be viewed in the context of the three types of information which exist on computers:

- Information for which access is open to the general public and permission is not required
- Information for which authorization is required and has been given; *i.e.*, username and password authentication
- Information for which authorization is required but has not been given (or, in the case of the prohibition on exceeding authorized access, has not been given for the part of the system accessed.)

According to the Ninth Circuit, the information which hiQ accessed and "scraped" fell into the first category of "computer information" for which no permission was required. As such, the court found that liability under the CFAA could not be based on LinkedIn's digital user agreement or the express revocation of hiQ's access rights contained in LinkedIn's cease-and-desist letter.[8]

The Renewed Importance of Requiring Password Authentication of Customer/User Data for CFAA Liability

The Ninth Circuit's decision underscores the importance of user authentication systems in determining whether liability under the CFAA will be triggered. In *U.S. v. Nosal*, 844 F.3d 1024 (9th Cir. 2016) ("*Nosal II*"), the Ninth Circuit held that a former employee whose computer access rights had been terminated when he left his employer, but who had then used current employees' login credentials to access company computers and collect confidential information, had acted "without authorization" in violation of the CFAA. Nosal II, 844 F.3d at 1038. Similarly, in *Facebook v. Power Ventures, Inc*, 844 F.3d 1058 (9th Cir. 2016), the Ninth Circuit held that Power Ventures, a social networking website that aggregated social networking information from multiple platforms, had violated the CFAA by accessing Facebook users' password-protected data (e-mail/contact information) and then using that data to send mass e-mail messages as part of a promotional campaign. *Id.* at 1062-63.

Using its newly-articulated analytical framework, the Ninth Circuit in *hiQ Labs* observed that, unlike LinkedIn users' public profiles, the computer information being accessed in *Nosal II* and *Power Ventures* was "plainly" the type where authorization was generally required; *i.e.*, requiring password authentication, and that authorization had either never been given or had been revoked:

> 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. The data hiQ seeks to access is not owned by LinkedIn and has not been demarcated by LinkedIn as private using … an [username/password] authorization system.[9]

Stay Tuned: LinkedIn's Petition for Rehearing and Rehearing En Banc

On October 11, 2019, LinkedIn filed its Petition for Rehearing and Rehearing En Banc, seeking reversal of the three-judge's panel's September 9th decision.[10]

While the outcome on LinkedIn's Petition is uncertain, one thing remains clear: the battle between SMC's and "scrapers" is far from over. Even if the panel's September 9th opinion remains intact, the Ninth Circuit made clear that SMCs and other online entities which view themselves as victims of data scrapping are not without legal recourse, noting that common law claims (e.g., trespass to chattels, unjust enrichment, conversion, breach of contract, and breach of privacy) and statutory claims (e.g., copyright infringement and misappropriation of trade secrets) may still be available.[11]

[1] *See, e.g., TicketMaster.com v. Tickets.com*, 2003 WL 21406289 (C.D. Cal. March 7, 2003) (dismissing copyright and trespass to chattels claims where only factual, publicly-available data was "scraped" from TicketMaster's website and re-published by Tickets.com in a different format, and Tickets.com's use of web crawler did not impact or interfere with the functionality of Ticketmaster.com's server); *Sandvig v. Sessions*, 315 F.Supp.3d 1 (D.D.C. 2018) (First Amendment interests were implicated and thus called into question the criminal prosecution of journalists under the Computer Fraud and Abuse Act for their use of automated bots to scrape data in breach of a website's terms of use agreement).

[2] -- F.3d --, 2019 WL 4251998 (9th Cir. Sept. 9, 2019).

[3] *Id.* at *9 (observing that LinkedIn's conduct "may well not be 'within the realm of fair competition.') (citations omitted).

[4] *See Alliance for the Wild Rockies v. Cottrell*, 632 F.3d 1127, 1131 (9th Cir. 2011) (adopting a sliding scale approach and holding that where the party seeking an injunction establishes irreparable harm is virtually certain, it need only demonstrate that there are "serious questions going to the merits" of its legal claims).

[5] -- F.3d --, 2019 WL 4251998 at * 5-6.

[6] *HiQ Labs v. LinkedIn Corp.*, 273 F.Supp.3d1099, 1110 (N.D. Cal. 2017).

[7] *Id.* at 1112.

[8] *Id.* at *12.

[9] -- *F.3d* --, 2019 WL 4251998 at *14.

[10] *HiQ Labs v. LinkedIn Corp.*, Case No. 17-16783 (9th Cir.), Dkt No. 82.

[11] *Id. (citing Associated Press v. Meltwater U.S. Holdings, Inc.*, 931 F.Supp.2d 537, 561 (S.D.N.Y. 2013) (holding that a software company's conduct in scraping and aggregating copyrighted news articles was not protected by fair use)).

Survey of Federal Courts of Appeals Cases Addressing Applicability of Anti-SLAPP Statutes in Federal Court

Wesley Lewis, Thomas J. Williams

Wesley Lewis

Thomas J. Williams

As more and more states adopt anti-SLAPP statutes, one question frequently facing litigants is whether, in a case brought in federal court in which jurisdiction is based on diversity of citizenship, the state anti-SLAPP statute applies. With seven of the twelve U.S. Courts of Appeals having now addressed the question, the answer seems clear: it depends. For practitioners trying to determine the applicability of an as-yet untested state statute, the analysis will require a careful reading of the specific state statute in question.

The starting point of the analysis, of course, is the *Erie* doctrine and the long-recognized principle that federal courts sitting in diversity "apply state substantive law and federal procedural law." *Hanna v. Plumer*, 380 U.S. 460, 465 (1965). But, as the Fifth Circuit recently noted in holding that the Texas statute, at least as it was written prior to September 1, 2019, is not applicable in federal court, "[d]etermining whether the state law is procedural or substantive may prove elusive." *Klocke v. Watson*, 936 F.3d 240, 244 (5th Cir. 2019). A summary of the Courts of Appeals decisions to date illustrates the difficulty in answering that "elusive" question.

Three Circuits have held that a state anti-SLAPP statute *does* apply:

First Circuit: In 2010, the First Circuit held that Maine's anti-SLAPP statute applies in federal court, concluding that there was no conflict between Federal Rule 12 motions to dismiss and anti-SLAPP motions. *Godin v. Schencks*, 629 F.3d 79, 86–87 (1st Cir. 2010). In reaching this conclusion, the Court noted that the purpose of anti-SLAPP motions are more limited, and that "Rules 12(b)(6) and 56 do not purport to apply only to suits challenging the defendants' exercise of their constitutional petitioning rights." *Id.* at 88. Additionally, the Court noted that Rule 12 and the special motion set forth in the Maine statute are both "mechanisms to efficiently dispose with meritless claims before trial," but that given the differences in mechanisms for dismissal and procedural burdens, Rule 12 motions and anti-SLAPP motions could "exist side by side," and that each motion could "control[] its own intended sphere of coverage. *Id.* at 91.

Second Circuit: In *Adelson v. Harris*, the Second Circuit approved the use of Nevada's anti-SLAPP statute in federal court in part because "immunity" and fee-shifting statutes are substantive under *Erie*. 774 F.3d 803, 809 (2d Cir. 2014). The Court in *Adelson* explained that "[e]ach of these rules [in Nevada's anti-SLAPP statute] (1) would apply in state court had suit been filed there; (2) is substantive within the meaning of *Erie*, since it is consequential enough that enforcement in federal proceedings will serve to discourage forum shopping and avoid inequity; and (3) does not squarely conflict with a valid federal rule. *Id*.

The Second Circuit similarly applied California's anti-SLAPP statute in federal court in *Liberty Synergistics Inc. v. Microflo Ltd.*, 718 F.3d 138 (2d Cir. 2013).

Ninth Circuit: The California anti-SLAPP statute, often used as a model for other states considering such statutes, was found to be applicable in federal court in *Newsham v. Lockheed Missiles & Space Co.*, 190 F.3d 963 (9th Cir. 1999). However, the Ninth Circuit only addressed two provisions at issue: the special motion to strike, and the availability of fees and costs. The Court "conclude[d] that these provisions and [Federal] Rules 8, 12, and 56 'can exist side by side … each controlling its own intended sphere of coverage without conflict.'" *Id*. at 972. The Court further opined that even though "the Anti–SLAPP statute and the Federal Rules do, in some respects, serve similar purposes, namely the expeditious weeding out of meritless claims before trial . . . [t]his commonality of purpose . . . does not constitute a "direct collision." *Id*.

Four Circuits have held that a state anti-SLAPP statute does *not* apply:

Fifth Circuit: In the most recent case addressing the question, the Fifth Circuit concluded that the Texas Citizens Participation Act (TCPA), Texas' anti-SLAPP statute, does not apply in federal court. *Klocke v. Watson*, 936 F.3d 240, 245 (5th Cir. 2019). The Court concluded that Federal "Rules 12 and 56, which govern dismissal and summary judgment motions, respectively, answer the same question as the anti-SLAPP statute: what are the circumstances under which a court must dismiss a case before trial?" and, accordingly, "because the TCPA's burden-shifting framework imposes additional requirements beyond those found in Rules 12 and 56 and answers the same question as those rules, the state law cannot apply in federal court." *Id*.

However, the Fifth Circuit appears to have also held that Louisiana's anti-SLAPP law could still apply in federal court. In *Henry v. Lake Charles American Press, L.L.C.*, 566 F. 3d 164 (5th Cir. 2009), the Court held that Louisiana's "nominally procedural" anti-SLAPP statute applies in federal court pursuant to the Erie doctrine. 566 F.3d 164, 169 (5th Cir. 2009). In *Klocke*, the Fifth Circuit distinguished the Texas and Louisiana statutes, noting that the TCPA differed from Louisiana's statute because it "imposes higher and more complex preliminary burdens on the motion to dismiss process and imposes rigorous procedural deadlines," *Klocke*, 936 F.3d at 248, thus leaving open the possibility that Louisiana's statute could still apply in federal court.

Tenth Circuit: The Tenth Circuit held that New Mexico's anti-SLAPP statute did not apply in federal court in *Los Lobos Renewable Power, LLC v. Americulture, Inc*, 885 F.3d 659 (10th Cir. 2018). The Court determined that the New Mexico statute provided a procedural mechanism designed to expedite the disposal of frivolous lawsuits but did not set forth any rules of substantive law; instead, the statute only affects the timing of disposition of SLAPP suits. "Unlike many other states' anti-SLAPP statutes that shift substantive burdens of proof or alter substantive standards, or both, under no circumstance will the New Mexico anti-SLAPP statute have any bearing on the suit's merits determination." *Id*. at 670 (citing *Makaeff v. Trump Univ., LLC*, 715 F.3d 254 (9th Cir. 2013) (addressing a California anti-SLAPP statute that shifted substantive burdens and altered substantive standards)).

Eleventh Circuit: In *Carbone v. Cable News Network, Inc.*, 910 F.3d 1345 (11th Cir. 2018), the Eleventh Circuit held that Georgia's anti-SLAPP statute did not apply in federal court, concluding that the motion-to-strike provision of the Georgia statute "answer[s] the same question" as [Federal] Rules 8, 12, and 56, but it does so in a way that conflicts with those Rules by requiring the plaintiff to allege and prove a probability of success on the merits. *Id*. at 1350. The Court held that the Rules "express 'with unmistakable clarity' that proof of probability of success on the merits 'is not required in federal courts' to avoid pretrial dismissal, and that the evidentiary sufficiency of a claim should not be tested before discovery. But the relevant provisions of the Georgia anti-SLAPP statute explicitly require proof of a probability of success on the merits without the benefit of discovery. The result is a 'direct collision' between the Federal Rules and the motion-to-strike provision of the Georgia statute." *Id*. at 1351 (internal citations omitted).

DC Circuit: The District of Columbia anti-SLAPP statute cannot be used in diversity cases in federal court. In *Abbas v. Foreign Policy Group, LLC, et al*., No. 13-7171 (D.C. Cir. Apr. 24, 2015), then-Judge (and future Supreme Court Justice) Brett Kavanaugh wrote that "[a] federal court exercising diversity jurisdiction should not apply a state law or rule if (1) a Federal Rule of Civil Procedure 'answer[s] the same question' as the state law or rule and (2) the Federal Rule does not violate the Rules Enabling Act." *Id*. (quoting *Shady Grove Orthopedic Assocs., P.A. v. Allstate Ins. Co.*, 559 U.S. 393, 398–99, 130 S. Ct. 1431, 1437 (2010) (majority op.)).

So far, the Courts of Appeals for the Third, Fourth, Sixth, Seventh and Eighth Circuits have not yet addressed this question. When they are presented with the opportunity to do so, predicting the outcome of those cases will require a careful reading of the exact language of the applicable state statute before them.

Haynes and Boone's Media, Entertainment and First Amendment Practice Group has extensive experience representing major media clients across all platforms – including newspapers, magazines, broadcast and cable networks, production companies, and online content providers – in high-profile disputes. Our team brings deep knowledge to a broad range of matters, including libel, intellectual property, and access to information. Our lawyers present frequently on issues facing the industry and have been leaders in drafting legislation to address cutting-edge issues affecting free speech and transparency.

FEATURED SPEAKING ENGAGEMENTS

Laura Prather

ABA Forum on Communications Law 25th Annual Conference
Panelist: Media Advocacy Workshop Panel Discussion of the Texas Citizens Participation Act
February 6, 2020
Austin, Texas

ABA Forum on Communications Law 25th Annual Conference
Facilitator: Hot Issues in Anti-SLAPP and Other Legislation Workshop
February 7-8, 2020
Austin, Texas

Thomas J. Williams

Texas Association of Broadcasters
Speaker: Southwest Broadcast Newsroom Workshop
November 16, 2019
Arlington, Texas

ABA Forum on Communications Law 25th Annual Conference
Facilitator: Hot Issues in Ethics
February 7-8, 2020
Austin, Texas

University of Texas School Law Conference
Speaker: Defamation Claims in the School Setting
February 21, 2020
Austin, Texas

RECENT RECOGNITIONS

Free-Speech Advocate Laura Prather Named Finalist for Professional Excellence in Advocacy Awards

Partner **Laura Prather** has been named a finalist for the Professional Excellence in Advocacy Awards for her work to support the Protect Free Speech Coalition and the Texas Citizens Participation Act (TCPA).

Haynes and Boone Featured in 2020 Best Lawyers in America Guide

Laura Prather: Litigation – First Amendment
Thomas J. Williams: Commercial Litigation, Litigation – First Amendment, Litigation – Intellectual Property
Catherine Robb: Litigation – First Amendment

Seven Haynes and Boone Lawyers Named 2020 "Lawyers of the Year"

Laura Prather: Litigation – First Amendment

Haynes and Boone Lawyers to be Honored with Texas Civil Rights Project Pro Bono Award

Wesley Lewis selected by the Texas Civil Rights Project (TCRP) to receive the Kristi Couvillon Pro Bono Award.

FOR MORE INFORMATION CONTACT:

LAURA LEE PRATHER
PARTNER
laura.prather@haynesboone.com
+1 512.867.8476

TOM WILLIAMS
PARTNER
thomas.williams@haynesboone.com
+1 817.347.6625