

# hiQ v. LinkedIn Redux? Ninth Circuit Decision Tested in New Case

**New Media and Technology Law Blog** on **September 27, 2019**

The ink is barely dry on the [landmark Ninth Circuit \*hiQ Labs\* decision](#). Yet, a new dispute has already cropped up testing the bounds of the CFAA and the ability of a platform to enforce terms restricting unauthorized scraping of social media content. (See [Stackla, Inc. v. Facebook, Inc.](#), No. 19-5849 (N.D. Cal. filed Sept. 19, 2019)). This dispute involves Facebook and a social media sentiment tracking company, Stackla, Inc., which, as part of its business, accesses Facebook and Instagram content. This past Wednesday, September 25th, the judge in the case [denied](#) Stackla, Inc.'s request for emergency relief restoring its access to Facebook's platform. While the judge has yet to issue a written ruling, the initial pleadings and memoranda filed in the case are noteworthy and bring up important issues surrounding the hot issue of scraping.

The Stackla dispute has echoes of *hiQ v. LinkedIn*. Both involve the open nature of "public" websites (although the "public" nature of the content at issue appears to be in dispute.) Both disputes address whether the Computer Fraud and Abuse Act (the "CFAA") can be used as a tool to prevent the scraping of such sites. Both disputes address how a platform may use its terms of use to prohibit automated scraping or data collection beyond the scope of such terms, although the discussion in *hiQ* was extremely brief. And like *hiQ*, Stackla asserts that if not for the ability to use Facebook and Instagram data, Stackla would be out of business. Thus both disputes address whether a court's equitable powers should come into play if a platform's termination of access will result in a particular company's insolvency. Given the Ninth Circuit's opinion in favor of *hiQ*, it is highly likely that Stackla's lawyers believed the Ninth Circuit decision was their golden ticket in this case. The judge's ruling on the request for emergency relief suggests they may be disappointed.

Stackla collects social media content on behalf of brands. Facebook offers an application program interface (an “API”) to allow third party developers to access Facebook and Instagram content. In May 2019, Stackla was approved as an Official Facebook Marketing Partner (FMP) after an extensive review of its business and advertising practices, giving it what it considered a stamp of approval as a vetted partner that met “the highest standards of performance.”

After an online news organization published articles that questioned the scraping practices of certain companies including Stackla, Stackla denied the allegations. Notwithstanding the denials, Facebook sent a cease and desist letter claiming that Stackla had, among other things, violated the CFAA and California state law equivalent (the California Computer Data Access and Fraud Act (“CDAFA”)) as well as Facebook’s and Instagram’s terms, and subsequently revoked Stackla’s access to Facebook and Instagram. [The revocation came in the midst of [Facebook’s recent push in the wake of the Cambridge Analytica incident to suspend apps](#) that purportedly misuse user data. (See a further explanation on [Facebook’s blog](#))]. Following termination of Stackla’s access, the parties engaged in some back and forth about Stackla’s applications, and Facebook requested extensive technical documentation about Stackla’s methods of accessing Facebook content. Such discussions ultimately did not lead to a resolution.

Three weeks after it had been denied access to Facebook and Instagram, Stackla filed a declaratory judgment action seeking a ruling that it has not violated the CFAA or CDAFA and that because its business model depended heavily on the use of public Facebook and Instagram data, a denial of access would bankrupt the company, leading to irreparable harm. Stackla also advanced claims for intentional interference with contract, unfair competition and breach of contract with respect to Stackla’s FMP status and its use of the API, among others. The complaint was filed just ten days after the Ninth Circuit issued its decision in *hiQ*.

Along with the complaint, Stackla also filed its motion for a temporary restraining order to compel Facebook to reinstate its access to the API. In a supporting [declaration](#), Stackla stated that it didn’t scrape data and did not access private social media content (visible only to “friends”), but acquired “approved or publicly available data” with permission via the Facebook API.

On September 23, 2019, Facebook filed its [opposition](#) to the TRO request, telling a different tale of Stackla's data practices. According to Facebook, Stackla did indeed engage in web scraping activities and that its business model was based, at least in part, on practices that sought to "evade" Facebook's terms prohibiting automated scraping. In its opposition papers, Facebook alleged Stackla had been accessing and saving public Instagram posts at a rate that indicated unauthorized scraping was occurring beyond the use of the API, thereby prompting Facebook to investigate and then terminate Stackla's access. Facebook professed a full-throated defense of what it termed "platform enforcement authority," or the right of any online service to combat unauthorized data scraping that violates its terms:

"It is common sense that Facebook should be able to enforce its own policies—including to revoke access to user data altogether for developers that fail to abide by Facebook's policies. It is also common sense that developers that violate Facebook's policies cannot just show up on the courthouse steps and demand that their access be reinstated."

On September 25, 2019, the court [denied Stackla's TRO request](#). A written order will be issued in the future.

The thrust of Facebook's defense to the TRO request rested, for the most part, on its right to enforce its terms and Stackla's alleged failure to document irreparable harm or a likelihood of success on the merits of its contract-related claims.

Facebook's opposition did not spend much time on the CFAA issue, with only a few citations to the Ninth Circuit's *hiQ* decision in distinguishing it from the facts of this dispute. Facebook argued that the current dispute is "nothing like *hiQ Labs*" for several reasons: (1) there was an ongoing contractual relationship between Stackla and Facebook (the Ninth Circuit questioned, in dicta, whether LinkedIn could enforce its user agreement against hiQ after its user status was terminated); and (2) unlike in *hiQ*, where the plaintiff claimed that LinkedIn's termination of hiQ's access had an implicit anti-competitive purpose, Stackla and Facebook are not in competition.

Facebook addressed the *hiQ* court's analysis of the CFAA issue in an interesting footnote in its opposition to the TRO:

“As for *HiQ*’s holding regarding the application of the CFAA to so-called publicly available data, the time to seek further review of that decision has not yet run. It would thus be especially imprudent to ‘declare’ the rights of the parties in this case under a decision that may well change.”

Moving the focus away from the CFAA, Facebook’s opposition summed up *hiQ* this way:

“The lesson of *HiQ*, then, is that online service providers, like Defendants, can and should stand on their ***contractual*** rights to prevent precisely the sort of conduct at issue here.” [emphasis original]

Interestingly, Facebook closed its argument by contending that a TRO compelling it to restore Stackla’s access would not be in the public interest, plainly making clear its stance against unwanted scraping that violates its policies:

“There is no public interest in forcing a technology company to do business with a web scraper. Rather, the public interest is served more meaningfully by permitting the Facebook to take all necessary steps to protect user privacy, including by enforcing against violations of their Terms....”

Given [Facebook’s success in alleging CFAA violations in the past](#), one wonders whether the foregoing statements by Facebook are meant to be a warning that third parties should not view the *hiQ* decision as a green light for scraping.

We will continue to follow developments in this case concerning the merits of Stackla’s claims and its request for injunctive relief (Stackla’s complaint asked for a preliminary injunction compelling Facebook to restore its access, so the parties may yet re-litigate this issue before the court). We will also be following the active *hiQ* litigation, where the Ninth Circuit will decide whether to rehear the case en banc. Beyond the CFAA-public website content issue, which took center stage in *hiQ*, the multiple contractual and equitable issues in the *Stackla* case make it a potentially important case for determining to what extent a platform that hosts publicly available user content may govern scraping.

[View Original](#)

[Related Professionals](#)

---

- **Jeffrey D. Neuburger**

Partner