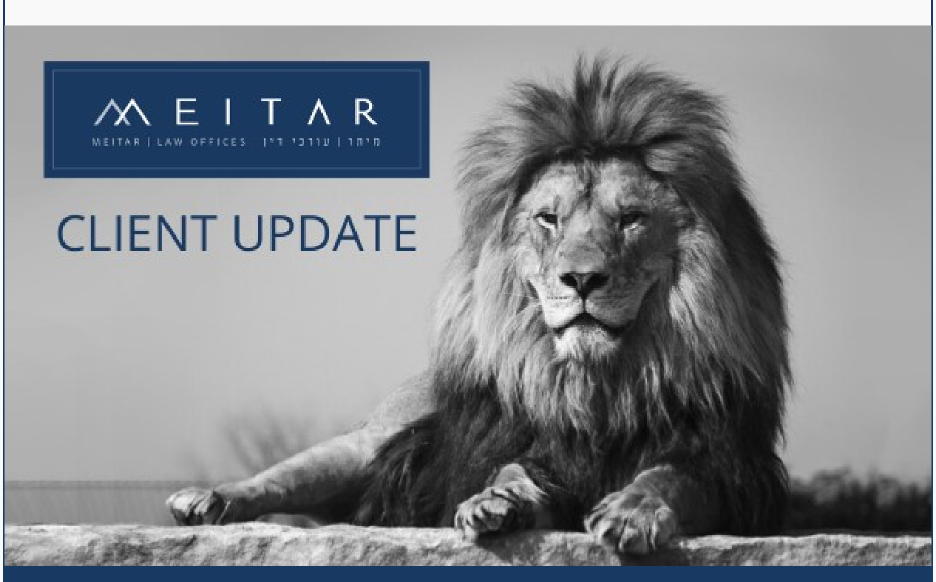
View this email in your browser



Not Even a Close Scrape: hiQ Wins Important Data Scraping Case Against LinkedIn

May 16, 2022

In the long-awaited decision in *hiQ Labs, Inc. v. LinkedIn Corp*.[1], the Ninth Circuit Court of Appeals ruled unanimously that automated scraping of publicly accessible data does not violate the Computer Fraud and Abuse Act ("CFAA"). Even if the Terms of Use of the website prohibit scraping—which is a common provision in Terms of Use—and even if a user has received a cease and desist letter informing them that they are not permitted to scrape data, a user's scraping is not a violation of the CFAA.

This is in contradiction to the holdings of several other circuit courts. The Ninth Circuit in *hiQ* held, however, that it "would attach criminal penalties to a breath taking amount of commonplace computer activity" if scraping were prohibited.

The Circuit Court adopted a very clear "gates-up-or-down" analysis of the CFAA. If the gates are "up" by permitting public access without username and password protection, the site cannot selectively prevent access to this public data.

This is a critical victory for the many businesses which scrape publicly available data from websites as a central part of their business model, as well as academics and journalists which analyze large amounts of public data. The question in the future will be whether the holding will be construed broadly to permit scraping on a wide scale, or whether it will be circumscribed to certain specific facts of this case.

Based on the combination of the *LinkedIn* case and Israeli cases, a few of which we note below, there are strategies that companies which wish to scrape should employ, and how they should design their business models going forward; conversely, these cases also present a road map for companies which wish to protect their sites from scraping how best to go about it.

1. The Facts- and Procedural History

Using automated bots, hiQ scrapes information that LinkedIn users have included on their public LinkedIn profiles. hiQ uses this data to create two products—"Keeper", which notifies employers which of their employees are at the greatest risk of being recruited away; and "Skill Mapper", which provides a summary of the skills possessed by individual workers.

LinkedIn sent hiQ a cease-and-desist letter in May 2017, demanding that hiQ stop accessing and copying data from LinkedIn. hiQ filed suit, seeking injunctive relief based on California law and a declaratory judgment that LinkedIn could not lawfully invoke the CFAA, the Digital Millennium Copyright Act, California Penal Code § 502(c), or the common law of trespass to prevent its scraping.

The district court found in favor of hiQ, and granted the preliminary injunction in August 2017. In September, 2019, the Circuit Court affirmed, and concluded that hiQ established a likelihood of irreparable harm because the survival of its business was threatened. The Circuit Court held that the district court did not abuse its discretion in balancing the equities and concluded that, even if some LinkedIn users retain some privacy interests in their information notwithstanding their decision to make their profiles public, those interests did not outweigh hiQ's interest in continuing its business. Thus, the balance of hardships tipped decidedly in favor of hiQ.

The Circuit Court further held that hiQ raised serious questions regarding the merits of (i) its claim that LinkedIn interfered with its contracts with third parties; (ii) its claim that the CFAA cannot be used to prevent hiQ's scraping; and (iii) LinkedIn's legitimate business purpose defense.

LinkedIn appealed the Circuit Court's decision to the Supreme Court, which ruled in June 2021 that the Ninth Circuit should review its holding again in light of the Supreme Court's decision on the CFAA earlier that month in *Van Buren v. United States.*

Now, the new decision issued by the Ninth Circuit in April, 2022, affirms the preliminary injunction against LinkedIn, thus preventing LinkedIn from blocking hiQ's scraping of publicly accessible profiles. Below we discuss the main holdings of this new decision.

2. The Circuit Court Opinion

The Circuit Court began by reviewing the district court's standard for granting a preliminary injunction, which applied the following sliding scale approach: "*A plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest.*"[2], whereby the stronger showing of one element may offset a weaker showing of another.[3] The district court concluded that the balance of hardships tips sharply in hiQ's favor and therefore, hiQ only needed to demonstrate "serious questions going to the merits".

A. Irreparable Harm: Applying this test, the district court concluded, and the Circuit Court affirmed, that there was a likelihood of irreparable harm to hiQ if preliminary relief were not granted, in that the survival of its business was threatened. Moreover, the Circuit Court accepted hiQ's argument that without access to LinkedIn public profile data, hiQ will likely be forced to breach its existing contracts with clients such as eBay, Capital One and GoDaddy, and to pass up pending deals with prospective clients. Therefore, the harm hiQ faces absent a preliminary injunction is not purely hypothetical.

B. Balance of the Equities (Including Expectation of Privacy): The district court "balanced the interests of all parties and weighed the damage to each in determining the balance of the equities."[4] On hiQ's side of the scale is the harm of going out of business; and on the other side, LinkedIn asserted that the injunction threatens its members' privacy, and therefore puts at risk the goodwill LinkedIn has developed with its members. The district court did acknowledge that "the fact that a user has set his profile to public does not imply that he wants any third parties to collect and use that data for all purposes." But there was little evidence that LinkedIn users who choose to make their profiles public actually maintain an expectation of privacy with respect to the information that they post publicly, and the Circuit Court was doubtful that they do. LinkedIn's privacy policy clearly states that "any information you put on your profile and any content you post on LinkedIn may be seen by others" and instructs users not to "post or add personal data to your profile that you would not want to be public."

Therefore, it concluded that LinkedIn's interest in preventing hiQ from scraping users' profiles is not significant enough to outweigh hiQ's interest in continuing its business, which depends on accessing, analyzing, and communicating information derived from public LinkedIn profiles. Additionally, LinkedIn had no protected property interest in the data contributed by its users, as the users retain ownership over their profiles.

C. Likelihood of Success: Since hiQ established that the balance of hardships tips decidedly in its favor, the likelihood-of-success of the preliminary injunction inquiry focuses on whether hiQ has raised "serious questions going to the merits."[5] The district court determined that it had, and the Circuit Court affirmed. This is the heart of the Circuit Court's opinion. While LinkedIn asserted a number of justifications for its actions, it focused on the CFAA. This was a law passed in 1986, which provides that "whoever . . . intentionally accesses a computer without authorization or **exceeds authorized access**, and thereby obtains . . . information from any protected computer . . . shall be punished by fine or imprisonment". LinkedIn asserted that hiQ exceeded its authorized access to LinkedIn's computers, which store the data that members share on LinkedIn's platform. Thus, to scrape LinkedIn data, hiQ must access LinkedIn servers, which are "protected computers".

The Circuit Court explained that the pivotal CFAA question was whether, following hiQ's receipt of the cease-and-desist letter, any further scraping and use of LinkedIn's data was "without authorization" within the meaning of the CFAA.

The Circuit Court analyzed the CFAA and said that it was essentially an "anti-hacking statute". Since hiQ did not "break and enter" into LinkedIn's website (since the data was publicly available), the Circuit Court held that the concept of "without authorization" is inapt. The Circuit Court held that if LinkedIn were to prevent access via a "gates down" approach, such as password protection, then LinkedIn would have a valid CFAA claim for hacking. But that is not the case here.

The Circuit Court noted that other circuits have held that violating a cease and desist letter, or a site's terms of use have been held to "exceed authorization" and are a violation of the CFAA, but the Ninth Circuit stated that it is holding otherwise—that, in its view, this is not a violation of the CFAA.

D. Public Interest: Although the district court stated that there were significant public interests on both sides, it concluded that, on balance, the public interest favors hiQ's position since data scraping is a common method of gathering information, used by search engines, academic researchers, and many others. The Circuit Court agreed with the district court that giving companies like LinkedIn free rein to decide, on any basis, who can collect and use data (that the companies do not own, that they otherwise make publicly available to viewers, and that the companies themselves collect and use) risks the possible creation of information monopolies that would disserve the public interest.

3. Israeli Law Perspective

There have been Israeli cases involving scraping, but which were decided on different bases, including the well-known 2006 Supreme Court case in *Maariv v. All You Need,* where an aggregator job site, AllJobs.co.il copied the help wanted ads from the Maariv website. The Court permitted the scraping on the basis that the copied data was factual and not copyright protected, and the rights in the data belonged to the advertisers, the job seekers.

There have also been a handful of lower courts in Israel which have addressed similar questions, some finding against the scrapers. For example, in *Viton v. Margalit*, a privacy argument against a scraper was successful. The Small Claims Court in Beit Shemesh partially accepted a claim against a website operator that scraped ads from public websites and displayed them on his own website. The court ruled that the display on the defendant's website was done without obtaining consent from the original advertisers, and therefore it harms the original advertisers. Because the ads on the defendant's website included personal information, and because they remain published after the original ads were removed, the court determined that the defendant's publication of the ads amounted to a violation of privacy rights and harms the original publisher.

The *Margalit* court also found that the plaintiff's actions amounted to "unjust enrichment", and quoted from the *Aloniel v. Ariel McDonald* case, that "whoever makes commercial use of the name, image or voice of another without obtaining his consent, engaged in unjust enrichment."

4. Conclusions and Implications

The *LinkedIn* decision is a big win for businesses and data aggregators which access public data and use it to create their own services or products, as well as for academics and journalists. The question will be how broadly future cases apply this permission to scrape, and how much they restrict it to the facts of this case.

For example, LinkedIn's decision to send a cease-and-desist letter occurred within a month of the announcement by LinkedIn's CEO that LinkedIn planned to leverage the data on its platform to create a new product for employers with similarities to hiQ's Skill Mapper product. The Circuit Court stated that if companies like LinkedIn, whose servers hold vast amounts of public data, are permitted to selectively ban potential competitors from using public data, that might well result in unfair competition under state law. Accordingly, a question will be whether sites which are not planning competitive products will be given broader scope to prevent scraping.

Second, the Circuit Court emphasized that LinkedIn does not own this data. Accordingly, a question will be whether future courts will permit scraping of data which is public, but which, unlike LinkedIn data, is also owned by the scraped site.

Third, the Circuit Court was concerned that LinkedIn could become an information monopoly, which would disserve the public interest. Will the same strict standard apply to small companies which are scraped and do not have the realistic capability of becoming an information monopoly?

Fourth, the balance of hardship weighed against hiQ because this was their sole source of data. What if the scraped data is just one of many sources for a scraping company? What would happen in a case like this, where it would not put the company out of business, but just make the product less "data-rich"?

Fifth, on hiQ's claim of intentional interference with contracts, the Circuit Court noted that hiQ had existing contracts with large customers which it would likely be forced to breach. Will the permission to scrape also apply to start-ups which do not yet have existing contracts which would be breached?

Finally, the Circuit Court stated that entities that view themselves as victims of data scraping are not without resort, even if the CFAA does not apply. They could also have claims for state law trespass to chattels, copyright infringement, misappropriation, unjust enrichment, breach of contract, or breach of privacy. Time will tell whether any of these claims will really be upheld by a court or whether they will be seen to be preempted by the CFAA or the rationale in this case.

One thing is for sure—we have not heard the last word on scraping!

[1] Available here.
[2] Winter v. Nat. Res. Def. Council, Inc., 555 U.S. 7, 20 (2008)
[3] Am. Trucking Ass'n v. City of Los Angeles, 559 F.3d 1046, 1057 (9th Cir. 2009)
[4] The Wireless Ass 'n v. City of Berkeley, Calif., 928 F.3d 832, 852 (9th Cir. 2019)
[5] Alliance for the Wild Rockies, 632 F.3d at 1131

Contact Information

Elnatan Levenstein, Associate
+972-3-6142652
elnatanl@meitar.com

David Mirchin, Partner
+972-3-6103199
dmirchin@meitar.com

For additional information about our firm's Technology group, click here