MEITAR | LAW OFFICES
16 Abba Hillel Silver Road, Ramat Gan, 5250608, Israel
Tel. + 972 3 6103100 Fax. + 972 3 6103111 www.meitar.com

Taking a Swipe at Scraping: Practical Takeaways from *hiQ v. LinkedIn* and *Meta v. BrandTotal*

In a previous client update, we analyzed the unanimous April, 2022 ruling of the Ninth Circuit Court of Appeals in the long-running case of *hiQ Labs, Inc. v. LinkedIn Corp* (the "***April hiQ Decision***") that automated scraping of publicly accessible data does not violate the Computer Fraud and Abuse Act ("**CFAA**"). However, the court said that they were leaving the door open to other claims of LinkedIn such as breach of contract.

That door has now shut on hiQ.

On November 4, 2022, the District Court for the Northern District of California ruled in summary judgment that hiQ breached LinkedIn's Terms of Use, specifically the provisions prohibiting data scraping and creating fake profiles (the "***November hiQ Decision***"). In December 2022, the parties finally ended the long-running case, with hiQ agreeing that it would not use automated means to access or copy data from the LinkedIn platform; it would delete any LinkedIn data collected without LinkedIn's express permission; and it would pay $500,000 to LinkedIn.

In a different case, *Meta Platforms, Inc. v. BrandTotal Ltd.* ("***BrandTotal*** "), in June, 2022, two months after the *April hiQ Decision*, the Northern District Court of California issued a summary judgment opinion upholding the prohibition on scraping in the Facebook Terms of Use.

Due to the widespread use of scraping—a process of extracting information from a website using automated means--by many technology companies, we are setting forth below our takeaways from the combination of these two new cases--the *November hiQ Decision* and the *BrandTotal* Decision.

1. November hiQ Decision

Using automated bots, the now-defunct hiQ scraped information that LinkedIn users included on their public LinkedIn profiles. hiQ used this data to create two products—"Keeper," which notified employers which of their employees were at the greatest risk of being recruited away; and “Skill Mapper”, which provided 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. The litigation has been continuing since then, all the way up to the US Supreme Court and back down again.

In the most recent action, LinkedIn moved for summary judgment on its breach of contract claim due

to (1) hiQ's scraping of LinkedIn's site, and using the collected data to sell its products, and (2) hiQ's use of fake accounts as part of hiQ's scraping operation, all in violation of its Terms of UseUse.

- **Ambiguous terms of use**

hiQ argued that (1) LinkedIn's Terms of Use are ambiguous because of inconsistent provisions within the terms, and (2) the court should consider extrinsic evidence that LinkedIn did not enforce its Terms of Use.

The court denied hiQ's claims, ruling that the Terms of Use were unambiguous that scraping was not permissible. Accordingly, no extrinsic evidence (such as a failure to enforce the Terms) was relevant.

- **No liability for independent contractors**

hiQ also argued against liability for the contractors they hired (" **turkers**"), who created fake users on behalf of hiQ, claiming that (1) there is no evidence that the turkers scraped any profile information, (2) hiQ is not responsible for its independent contractors' acts, and (3) there is no evidence of actual harm to LinkedIn.

The court ruled with respect to these claims that "regardless of whether the turkers scraped LinkedIn's site, they breached the User Agreement prohibition on creating false identities", and that "although turkers were hiQ's independent contractors, hiQ cannot escape liability because they also acted as its agent … since hiQ retained a high degree of control over turkers".

- **No requirement of actual harm**

Additionally, with respect to hiQ's claim about actual damage, the court ruled that "nominal damages are available for breach of contract and can support entry of judgment in favor of a plaintiff who suffered 'no appreciable harm'".

To summarize, the court ruled that, "hiQ breached LinkedIn's terms both through its own scraping of LinkedIn's site and using that scraped data and through turkers' creation of false identities on LinkedIn's platform".

- **hiQ's affirmative defenses: waiver and estoppel**

hiQ also raised several affirmative defenses, including that LinkedIn waived its right to sue for breach of contract since it knew about hiQ's scraping and use of scraped data as early as 2014, and did not enforce its Terms of Use against hiQ, and similarly that LinkedIn is estopped from preventing hiQ from scraping because it acquiesced in hiQ's scraping over several years.

The court agreed that there was evidence that a jury could reasonably conclude that LinkedIn did not promptly pursue its rights, and that therefore it waived its rights to enforce its Terms of Use. Accordingly, it rejected LinkedIn's summary judgment on those issues.

The court did rule, however, that there is no evidence showing that LinkedIn knew about hiQ's use of turkers before this action. Therefore, LinkedIn did not waive its rights to enforce its Terms of Use prohibiting the creation of false accounts by the turkers.

To summarize, the court held that Terms of Use prohibiting scraping and creating fake accounts was enforceable. Because hiQ might, however, have a good affirmative defense that LinkedIn did not enforce the breach of contract promptly against the scraping activity, it denied LinkedIn's motion for summary judgment on the breach of contract claim regarding such scraping activity.

2. *BrandTotal* Decision

BrandTotal provided advertising consulting services to corporate clients regarding how the digital advertisements of those clients and their competitors are presented to social media users. The primary product at issue in this case was a browser extension called UpVoice.

After successfully petitioning Google to remove UpVoice from its online store, Meta filed claims against BrandTotal in California on October 1, 2020, claiming that BrandTotal's practices violated (a) the CFAA, (b) the state law equivalent of the CFAA, the California Comprehensive Computer Data Access and Fraud Act ("**CDAFA**"), and (c) Facebook's Terms of Use, which prohibited scraping.

Eventually, both BrandTotal and Meta moved for a summary judgment. BrandTotal sought summary judgment on Meta's contract claim based on two defenses:

(a) Facebook's Terms of Use prohibiting scraping violates public policies related to data ownership, market competition, and the free flow of information and speech; and

(b) certain provisions of the Facebook Terms of Use are unconscionable.

- **Privacy Claims**

BrandTotal argued that the California Consumer Privacy Act ("**CCPA**") and the California Privacy Rights Act ("**CPRA**") embody a principle of user control over data sufficient enough to invalidate Facebook's Terms of Use.

The court did not agree; it dismissed these claims because BrandTotal did not cite any substantive provision of the CCPA or the CPRA that prevents Meta from enforcing its Terms of Use.

- **Public Policy/Competition Claims**

In addition, BrandTotal argued that prohibiting unauthorized automated access violates public policies, including that of promoting market competition.

However, the court ruled that antitrust law permits market participants to refuse to deal with competitors, and BrandTotal failed to provide plausible allegations of a product market, market power, or any other basis for an exception to this rule. The court went to lengths to emphasize that BrandTotal did not offer meaningful economic analysis of the market, each party's market share, whether there were substitutes for the data that BrandTotal collected from Meta, whether the data collected from scraping Facebook ads was needed in order to compete, and, most importantly, the evidence that would support their allegations. Mere allegations were not enough.

- **Free Speech Claims**

BrandTotal also argued that Facebook's Terms of Use violate public policy since it "impermissibly burdens interests in free speech and the flow of information, rooted in the First Amendment to the U.S. Constitution and … the California Constitution". The court ruled that the effect of the access restriction on the free speech and the flow of information was not clear, and dismissed this claim.

- **Unconscionability Claims**

Finally, BrandTotal claimed that Facebook's Terms of Use are unconscionable and therefore the anti-scraping provision is unenforceable, specifically because: (a) certain user restrictions survive beyond the termination of an account; and (b) Meta's limitation of liability is no more than the greater of $100, or the amount the user has paid Meta in the previous year.

In order to render a contract unenforceable under the doctrine of unconscionability, there must be both a procedural and substantive unconscionability.

- **Procedural Unconscionability**

The court ruled that BrandTotal was offered Facebook's terms on a take-it-or-leave-it basis, with no power to negotiate. Therefore, Facebook's Terms are "procedurally unconscionable in that they represent a contract of adhesion".

- **Substantive Unconscionability**

However, with respect to the specific provisions, "BrandTotal has not shown that any public policy implication of section 3.2.3 [prohibiting scraping] meets the high standard of substantive unconscionability". As for the limitation of liability claim, the court concluded that "if the limitation of liability is unconscionable, the appropriate course would be to decline to enforce that provision, not

any other provision (like section 3.2.3) that confers rights or obligations on either party from which liability might arise".

- **CFAA and CDAFA Claims**

The *BrandTotal* court continued with the approach taken in the *April hiQ Decision* that scraping publicly available data is not a violation of the CFAA. (In a different context, the Supreme Court in *Van Buren* also restricted the scope of the CFAA). The court in *BrandTotal* emphasized that the CFAA was a statute aimed at preventing hacking and therefore, where a website is made available to the public without password protection or any other authentication requirement, it is not a violation of the CFAA's prohibition of accessing websites "without authorization", even if the owner of the website, such as Meta here, revoked a user's access or employed technological measures to block a user.

Therefore, the court held that BrandTotal did not violate the CFAA or the CDAFA when it accessed non-password-protected pages. In contrast, the court ruled in favor of Meta with respect to BrandTotal's access to password-protected pages, using fake user accounts, and held that this practice was in violation of the CFAA and the CDAFA.

3. **Key Takeaways and conclusions**

The earlier hiQ decisions made history by holding forcefully that scraping of publicly available websites was not a violation of the CFAA, and therefore, scrapers were not subject to the criminal liability under this statute. After the *April hiQ Decision*, it looked as if scraping might be broadly permitted as the court emphasized that the CFAA was intended to be primarily an anti-hacking statute. In the aftermath of *BrandTotal* and the *November hiQ Decision*, however, the courts have taken a much tougher stance against scraping.

The following are six main takeaways on the current state of the law:

1. <u>Upholding contracts prohibiting scraping.</u> Courts are likely to uphold provisions in Terms of Use prohibiting scraping.
    a. If your company wishes to prevent scraping, you should carefully review your Terms of Use to ensure that:
        i. they include a prohibition on scraping,
        ii. they are drafted in a manner which is not ambiguous, and
        iii. they are presented to users in a manner which will be enforceable.
    b. If your company is engaged in scraping, note that not all websites prohibit scraping. For example, US federal government websites containing essential data, such as clinical trial data, does not prohibit scraping.

2. Turkers Won't Help. You cannot avoid liability for scraping simply by hiring third party contractors—turkers—to scrape for you.
3. Act Promptly; Do Not Delay! If your company wishes to enforce a prohibition on scraping, you will need to take action promptly upon becoming aware of the scraping activity. LinkedIn was successful in blocking the use of fake accounts since it acted promptly once it became aware. On the other hand, LinkedIn knew about hiQ's scraping for quite a while before it took action. Therefore, the court stated that hiQ might have a good defense that LinkedIn waived its right by waiting so long to enforce its anti-scraping prohibition against hiQ.
4. Access Non-Password Protected Sites. If your company scrapes, it is not a violation of the CFAA if you are accessing sites which make data publicly available and do not protect it by password. If, on the other hand, your company wishes to retain the possibility of claiming that scrapers have violated the CFAA, you should design it with password-protection.
5. Personal Data Considerations. If the data your company scrapes includes personal data, your company will need to ensure that it is in compliance with applicable privacy and data protection laws protecting that personal data, such as registering the database of personal data in Israel with the Database Registrar or notifying data subjects under the GDPR.
6. Not the Last Word. While the *BrandTotal* and *November hiQ Decision* provide certain guidance, there are other scraping cases making their way through the courts, such as *Ryanair DAC v. Booking Holdings* in Delaware District Court, which should augment the guidance. In addition, we will need to see how courts treat other common industry practices, such as collecting data for users who have voluntarily provided their credentials to another.

Bottom line: scraping continues to be a fluid area of the law, and we expect further cases, including in other circuits and other countries, that should shed light on which scraping practices are permitted and which are not.