THE
NATIONAL LAW REVIEW

Court Denies TRO against Data Scraper That Accessed Private Database via Registered Accounts

Thursday, June 21, 2018

Article By Proskauer Rose LLP
Jeffrey D Neuburger
New Media and Technology Law Blog

Communications, Media & Internet
Texas

This past week, a Texas district court denied a bid from a web service for a temporary restraining order (TRO) to enjoin a competitor that allegedly scraped a large amount of proprietary data from its closed site via several user accounts. (*BidPrime, LLC v. SmartProcure, Inc.*, No. 18-478 (W.D. Tex. June 18, 2018)). While tempting to draw a general legal conclusion about the permissibility of scraping from this decision, the decision was in fact based on the judgement of the court that scraping was unlikely to continue during the pendency of the litigation.

Nonetheless, the dispute highlights the host of legal issues that can arise when an entity accesses a website or database to scrape data for competitive or other reasons using user credentials or fake accounts or proxies to mask its true identity. For example, the plaintiff BidPrime, LCC ("BidPrime") sought injunctive relief based upon claims under the federal Computer Fraud and Abuse Act (CFAA) and state law counterpart, state trade secret law, and breach of contract, among others. Whether such claims are viable are of course dependent on the specific facts and circumstances of the dispute, the restrictions contained in the website terms of use,what countermeasures and demands the website owner made to the web scraper to prevent unwanted access, and the state of the current interpretation of applicable law. This decision did not analyze these factors beyond concluding that ongoing scraping was unlikely.

The plaintiff BidPrime developed software to monitor and collect bid requests and contracts issued by public and private entities and operated a closed website that allowed registered users to view the data. A competitor, SmartProcure, Inc., ("SmartProcure" or "Defendant") allegedly accessed BidPrime's proprietary database and scraped data using registered accounts (and also an account allegedly registered by a SmartProcure employee under a fake identity).

The court denied the TRO for several reasons. First, the court found that BidPrime failed to show a likelihood of success on the merits for its trade secret claim because it may not have taken sufficiently reasonable measures to protect its secret bid data because the version of the website terms in force did not contain any significant use restrictions or otherwise prohibit a user from making BidPrime's aggregation of bid data public information. As for the CFAA claim for unauthorized access – a typical claim in a web scraping dispute – the court ruled that BidPrime did not show irreparable harm, as the facts suggested that it was not likely that SmartProcure would access BidPrime's website during the litigation. For example, the court noted that SmartProcure offered plaintiff assurances that such access would no longer occur, SmartProcure stated it had imaged laptops that were allegedly used for the scraping and that plaintiff's security countermeasures have been shown effective at detecting or blocking several of SmartProcure's attempts to access the site. As it is still early in the litigation, it remains to be seen how the court will view the merits of the claims after the facts are more fully developed.

We have previously discussed the CFAA considerations of using sham accounts to extract data from a website for research purposes, as well as the Ninth Circuit's examination of the landmark *hiQ* decision, where a lower court had granted an injunction that limited the applicability of the CFAA to the blocking of an entity engaging in commercial data scraping of a public website. However, different considerations come into play when scraping a private website where data is only accessible to registered or paid accounts. Indeed, the issue of the scraping of data from private websites or apps for competitive reasons is an emerging issue, evidenced by another scraping-related suit filed this month concerning the alleged use of fake accounts to gain access.

(See Lemonade, Inc. v. One Versicherung AG, No. 18-5368 (S.D.N.Y. Complaint filed June 14, 2018) (insurer lodged CFAA and contract claims against a competitor for allegedly created fake accounts to access the insurer's app to extract data on pricing and claim procedures)).

Source URL: https://www.natlawreview.com/article/court-denies-tro-against-data-scraper-accessed-private-database-registered-accounts