Proskauer

CFAA "Unauthorized Access" Web Scraping Claim against Ticket Broker Dismissed Because Revocation of Access Not Expressed in Cease and Desist Letter

New Media & Technology Law Blog on **February 9, 2018**

A California district court issued an important opinion in a dispute between a ticket sales platform and a ticket broker that employed automated bots to purchase tickets in bulk. (*Ticketmaster L.L.C. v. Prestige Entertainment, Inc.*, No. 17-07232 (C.D. Cal. Jan. 31, 2018)). For those of us who have been following the evolution of the law around the use of automation to scrape websites, this case is interesting. The decision interprets some of the major Ninth Circuit decisions of recent memory on liability for web scraping. Indeed, two weeks ago, we wrote about a case in which the Ninth Circuit interpreted certain automated downloading practices under the CFAA and CDAFA. Also, we wrote about and are awaiting the decision in the *hiQ v. LinkedIn* appeal before the Ninth Circuit. Also prior posts on the topic include a discussion of a noteworthy appeals court opinion that examined scraping activity under copyright law and the scope of liability under the DMCA anticircumvention provisions. These seminal decisions and the issues they raise were expressly or implicitly addressed in the instant case. While we will briefly review some of the highlights of this decision below, the case is a must-read for website operators and entities that engage in web scraping activities.

Background

For the past two years, the defendant ticket brokers have allegedly been using bots and dummy accounts to navigate Ticketmaster's website and mobile app to purchase large quantities of tickets to popular events to resell for higher prices on the secondary market. To combat brokers, Ticketmaster employs various countermeasures, such as limiting purchases, regulating the speed users may refresh purchase requests, and installing various security measures to thwart bot activity, such as CAPTCHA. According to the complaint, in this case, defendants used colocation facilities with high speed bandwidth, random number and letter generators, and other evasive methods in order to avoid detection by Ticketmaster, as well as using automated means to bypass CAPTCHA screens and "CAPTCHA farm" laborers (overseas workers paid a small wage to click on and decipher CAPTCHA boxes).

As part of the ticket buying process, users must agree to Ticketmaster's terms of use before they can view and use Ticketmaster's website and mobile app. Users are also required to agree to a "Code of Conduct" in the terms and abide by purchasing limits. The terms also prohibit a number of automated activities, such as using robots, spiders, or automated tools to mine data, defeat CAPTCHA tools, or search for or purchase tickets, as well as any actions that impose an unreasonable large load on Ticketmaster's servers.

The Claims

Ticketmaster brought suit against the defendants alleging a variety of claims including copyright infringement and violation of the anticircumvention provisions of the Digital Millennium Copyright Act (part of the Copyright Act), state breach of contract, fraud and related claims, violation of the New York anti-ticket bot law, violation of the Computer Fraud and Abuse Act (CFAA), and violation of the California state Computer Data Access and Fraud Act (CDAFA). (Note: This suit came on the heels of a defendant's (Renaissance Ventures d/b/a Prestige Entertainment) $3.3 million settlement with the New York State Attorney General in May 2017 over alleged violations of New York's ticket laws and the use of illegal ticket bots.) In considering the defendant's motion to dismiss, the court allowed the plaintiff's DMCA anticircumvention claims as well as breach of contract, fraud and other related state law claims to go forward (the claim for civil violations of the New York anti-ticket bot law were not before the court), but dismissed claims under the CFAA and CDAFA (with leave to amend) as well the plaintiff's other claims. This blog post is intended to briefly summarize the court's analysis of the CFAA and DMCA issues.

The Ruling

Plaintiff alleged that the defendant violated the CFAA. The CFAA imposes liability on any party that "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains," *inter alia,* "information from any protected computer. In the Ninth Circuit's 2016 *Power Ventures*ruling, that panel held that an entity can run afoul of the CFAA when he or she has no permission to access a computer or when such permission has been revoked explicitly, but that a violation of the terms of use of a website, without more, cannot be the basis for liability under the CFAA. In this case, the issue was whether defendants lacked authorization when using Ticketmaster's website or apps. Ticketmaster contended that defendants lacked or exceeded their authorization by violating its terms, even after it sent defendants a cease and desist letter outlining the alleged violations. In dismissing the claim, the court found that Ticketmaster's cease and desist letter had "not shown that it rescinded permission from Defendants to use its website." However, since the court granted leave to amend the CFAA and CDAFA claims, Ticketmaster could state a viable claim by presenting evidence that, after it sent the cease and desist letter, it took steps to prevent defendants from future access to its networks by, for example, closing accounts or blocking IP addresses affiliated with defendants, or otherwise bolster its claims by alleging that defendants implemented "hacks" and "backdoors" to enable bots to gain access to Ticketmaster's systems to purchase tickets.

With respect to Ticketmaster's claims under copyright, while the court dismissed Ticketmaster's copyright infringement claims, it did allow Ticketmaster's DMCA claims to go forward. The DMCA provides that: "[n]o person shall circumvent a technological measure that effectively controls access to a [copyrighted] work." 17 U.S.C. § 1201(a)(1). To circumvent a technological measure means to "descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner." 17 U.S.C. § 1201(a)(3)(A). Such things as encryption measures and software activation and validation keys have been deemed technological measures within the meaning of the DMCA. In allowing the claim to go forward, the court stated that CAPTCHA was a technological measure under the DMCA, as it prevents a user from proceeding further to gain access to copyrighted pages, and that allegations that defendants used colocation facilities and other methods, such as deleting cookies, were also actionable under the DMCA if used to circumvent Ticketmaster's technological measures. This aspect of the ruling is important as the DMCA provisions allow for statutory damages "per act of circumvention" and, as it is a federal law claim, it allows the district court to retain jurisdiction over the dispute.

Despite trimming the causes of action in the complaint, the court granted leave to amend the CFAA and CDAFA claims. In any case, Ticketmaster's remaining claims are formidable. It will be interesting to see how this litigation proceeds, including how the court analyzes the DMCA and state law claims in the context of an unwanted network access dispute.

View original

Related Professionals

- **Jeffrey D. Neuburger**
  Partner