JULY 20, 2017

Legaltech© news

ONLINE

An ALM Publication

What Courts Have Said About the Legality of Data Scraping

Parties have sought to stop scrapers using a number of legal bases, from the CFAA to copyright law.

BY PAVEN MALHOTRA AND ANDREA NILL SANCHEZ, KEKER, VAN NEST & PETERS

As of 2015, nearly a quarter of all website visits are by data scrapers. Not only are the numbers even higher in some industries, they have likely increased. Given the enormous role scrapers play in internet traffic, it is critical to understand their role and the legal framework they operate in. This article—the first of a two-part series—explores the contours of scraping and the legal bases upon which parties have sought to stop scrapers.

What is Data Scraping?

Data scraping refers to the act of extracting large amounts of information from a website using automated software programs called "bots."

Although that may sound nefarious, often it is beneficial. Search engine companies engage in scraping that most websites welcome because they want internet users to be able to discover their information. Other types of web scraping services that promote access to information include targeted advertising, price aggregators, and personal finance management tools.

peterhowell

Data scraping isn't always bad, but it does have a darker side. Malicious hackers often use scraping tools to access and save sensitive financial and personal data. Data scraping can also be used as an anti-competitive tool.

Both "good" and "bad" data scraping may be unlawful in certain instances. And the penalties that result from a legal judgment can be severe. Earlier this year, Craigslist obtained a $60.5 million judgment against a company that it accused of scraping website content.

Litigating Data Scraping

Civil cases involving data scraping typically involve four different types of claims: (1) violations of the Computer Fraud and Abuse Act; (2) breach of contract; (3) trespass to chattel; and (4) copyright infringement. Since none of these statutes or doctrines was specifically conceived to address the practice, courts have had to cobble together a body of case law to fill the gaps.

CFAA

Congress passed the Computer Fraud and Abuse Act (CFAA) in 1986 to criminalize and provide civil remedies for accessing a computer without authorization or exceeding the scope of authorized access. Two cases illustrate the CFAA's potential and limitations in the data scraping context.

Craigslist obtained a CFAA victory against 3Taps, Inc., a company that provided an alternative user interface for accessing Craigslist's real estate listings. 3Taps argued that its access of Craigslist data was not "unauthorized" because the data was public. The Court rejected that position, holding that Craigslist had limited 3Taps access via cease and desist letters and blocking access from 3Taps' IP addresses. These measures rendered 3Taps' persistent access "unauthorized."

The Eastern District of Pennsylvania reached a different outcome in a suit filed by QVC against start-up Resultly under a different provision of the CFAA—one that prohibited the release of code which "intentionally causes damage without authorization" to a computer. Even though Resultly's crawling activities crashed QVC's website, QVC failed to show that it was Resulty's "conscious objective" to cause any harm.

These divergent results suggest CFAA cases often turn upon which provision of the Act a plaintiff sues under.

Breach of Contract

It turns out that the timeworn breach of contract claim is one of the most effective means for addressing data scraping. Nearly every major commercial website today deploys a terms of service as a condition to accessing material within the site. With the rise of scrapers, these agreements increasingly prohibit scraping. And for the most part, courts are willing to enforce them.

That is especially the case when a user assents to a "clickwrap" agreement, which requires affirmatively checking a box agreeing to abide by a website's terms.

Data scraping cases get more complicated when they involve "browsewrap" agreements that simply appear somewhere on the website. The fact that the agreement is available for review may not be enough to establish that the scraper actually saw and had notice of the terms.

Trespass to Chattels

Data scraping claims have also breathed new life into the tort of trespass to chattels, which imposes liability for an intentional and harmful interference with the possession of personal property.

The fact that the harm caused by data scraping may be difficult to quantify has not proved to be a barrier. In *eBay, Inc. v. Bidder's Edge, Inc.*, eBay successfully invoked the doctrine against an auction aggregation site. The Northern District of California court granted preliminary injunctive relief, citing eBay's claim that the defendant's unauthorized access used valuable bandwidth and capacity.

Copyright

In certain limited scenarios, a data scraper may also be liable for copyright infringement. In 2013, the Associated Press (AP) successfully alleged copyright infringement against the internet news clipping service Meltwater, which scraped and partially reproduced the AP's news content. The court found that AP established copyright infringement and rejected Meltwater's argument that its interactions with subscribers are equivalent to search engines.

But data scrapers usually aren't extracting copyrightable information. Only the tangible expression of an idea—not the idea itself—is protected.

Such was the case in a lawsuit brought by Ticketmaster against Tickets.com, a competing company that posted scraped ticket information. A Central District of California court found Tickets.com was only "[t]aking [a] temporary copy of the electronic information for the limited purpose of extracting unprotected public facts."

Given this legal backdrop, what measures can websites implement to discourage data scraping and what precautions can scrapers take to avoid litigation? Those steps will be the topic of the next article of this two-part series.

***Paven Malhotra** is a partner at Keker, Van Nest & Peters. He focuses his practice on litigating high-stakes business and intellectual property disputes. **Andrea Nill Sanchez** is an associate at Keker, Van Nest & Peters and counsels clients through complex patent disputes.*