WSGR ALERT

MAY 2010

OHIO DISTRICT COURT ALLOWS DATABASE "SCRAPING" CASE TO PROCEED ON A VARIETY OF LEGAL THEORIES

Recent years have seen the growth of online data sources, such as online databases, e-commerce catalogs, and social networking sites, and associated services and applications. This growth has been accompanied by a corresponding increase in the sophistication of technologies that automate access and retrieval of online data, a practice commonly referred to as "scraping."

The *Snap-On Bus. Solutions, Inc. v. O'Neil & Assoc., Inc.* case,[1] in which the plaintiff alleged a variety of claims that are typical in a scraping case, presents a timely opportunity to review the developing body of case law relating to automated access of third-party systems, including scraping and the use of third-party content. The plaintiff, Snap-On Business Solutions (Snap-On), survived a summary judgment motion and was allowed to proceed to trial on a variety of claims it brought against O'Neil & Associates (O'Neil) in the Northern District of Ohio, in connection with O'Neil's use of a scraping tool to access and replicate data from an online database built and hosted by Snap-On.

Snap-On initially created the searchable online database at issue for its client Mitsubishi, using data and images provided by Mitsubishi. Mitsubishi later decided to move the database to another service provider (O'Neil), but Snap-On refused to provide the database to Mitsubishi unless Mitsubishi paid an additional fee. Mitsubishi and O'Neil agreed that O'Neil would retrieve the data from Snap-On's database through the use of O'Neil's "scraper tool." O'Neil proceeded to scrape the data from the Snap-On database, simulating logins by Mitsubishi personnel using access credentials supplied by Mitsubishi. After experiencing performance issues with its service, Snap-On became aware of the scraping activity and filed suit.

Computer Fraud and Abuse Act

Snap-On alleged violations of the federal Computer Fraud and Abuse Act (CFAA), which provides civil and criminal penalties for accessing third-party computer systems without authorization (including by exceeding the scope of authorization). The court in *Snap-On* found that a material question of fact existed as to whether language in the contract between Snap-On and Mitsubishi making Mitsubishi responsible for "authorization security" and "assigning user names and passwords to authorized users" gave it the power to authorize a third party to access the online database, in light of other language suggesting that users had to be affiliated with Mitsubishi to be authorized.

In previous scraping cases, courts have allowed plaintiffs to proceed with CFAA claims on the grounds that scraping activity was "unauthorized" in light of provisions in a website's terms of service prohibiting automated access, commercial use of the website, or use on behalf of a third party.[2] Notably, all 50 states have enacted statutes addressing computer abuse and fraud, and unauthorized access, including California Penal Code §502(c).

Trespass to Chattels

The court next discussed Snap-On's common-law trespass to chattels claim, which requires a plaintiff to show that it was harmed by the defendant's interference with the use or possession of the plaintiff's personal property. The court first held that Snap-On's computer servers were personal property susceptible to a trespass claim.[3] Noting that courts in a variety of prior scraping cases have taken different positions on the form and substance of damages required to support the claim,[4]

---

[1] C 5:09-cv-01547-JG (N.D. Ohio, April 16, 2010).

[2] See, e.g., *Southwest Airlines v. Farechase*, 318 F. Supp. 2d at 439-40 (N.D. Texas, 2004).

[3] Citing *Compuserve, Inc. v. Cyber Promotions*, 926 F. Supp. 1015, 1021 (S.D. Ohio, 1997) and *Universal Tube & Rollform Equip. Corp. v. YouTube, Inc.*, 504 F. Supp. 2d 260, 268 (N.D. Ohio, 2007).

[4] Citing *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 404 (2d. Cir., 2004) (intangible damage capable of causing harm in the aggregate is sufficient); *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1071 (N.D. Cal., 2000) (scraping activity that interfered with plaintiff's ability to fully utilize servers for its own purposes is sufficient); *Intel Corp. v. Hamdi*, 71 P.3d 296 (Cal., 2003) (insufficient damage where plaintiff was not prevented from using its servers for a measurable length of time); and *Ticketmaster Corp. v. Tickets.com, Inc.*, No. 99CV7654, 2000 WL 1887522, at *4 (C.D. Cal., 2000) (insufficient damage where scraper used a small percentage of processing power, and plaintiff did not show actual interference with regular business operations).

Continued on page 2...

Ohio District Court Allows Database "Scraping" Case . . .

Continued from page 1...

the court held that a jury could find that the increased traffic from O'Neil's scraping constituted the requisite damage.

Unjust Enrichment

Snap-On also alleged that O'Neil obtained business benefits at Snap-On's expense, giving rise to an unfair competition claim for unjust enrichment. Unfair competition, a state-law claim, generally applies when (1) the plaintiff has invested substantial time and money in the development of its product; (2) the defendant has appropriated that product at little or no cost; and (3) the plaintiff has been injured by the defendant's conduct. The claim may, however, be preempted by copyright law when the misappropriated work falls within the subject matter of copyright.

The court in *Snap-On* found that Snap-On failed to identify the allegedly misappropriated "information" sufficiently to find that the claim was not preempted by copyright law. Snap-On's failure to allege misappropriation of specific, noncopyrightable data or information, combined with its allegations of copyright infringement claims (as discussed below), led the court to determine that no separate unjust enrichment claim could be supported.

Previous scraping cases have held that misappropriation of factual data, to which copyright protection does not extend, can support an unfair competition claim. For example, in *Southwest Airlines v. Farechase*, the plaintiff's unfair competition claim survived a motion for summary judgment where the defendant was displaying on its own website pricing data that it had scraped from Southwest's website, harming Southwest by drawing user traffic away from Southwest's website.[5]

Breach of Contract

Snap-On further asserted a breach of contract claim, based on its user agreement. The agreement was made available to users before logging in by means of a statement acknowledging that use of the service was subject to the terms of the agreement, and providing a link to the agreement. In allowing the claim to proceed to trial, the court cited a variety of prior cases from other jurisdictions holding this type of "browsewrap" agreement enforceable when the user had actual or constructive notice of the agreement prior to using the service.

Snap-On's user agreement conditioned the right to use the service on the user's status as a dealer or customer licensee, which O'Neil was not. However, the agreement also provided that the terms of a separate written agreement could supersede the browsewrap agreement. As Mitsubishi had such an agreement with Snap-On that could be interpreted to give Mitsubishi the right to authorize O'Neil to access the service, the court allowed the claim to proceed to trial.

Breach of contract claims based on a scraper's failure to adhere to the terms of a website terms of use agreement are commonly asserted by plaintiffs in scraping cases. Particular provisions of such agreements that have been invoked to challenge scraping include prohibitions on (1) access to the service or use of content available through the service other than for personal, noncommercial purposes; (2) circumvention of security features (such as robots.txt files, CAPTCHA challenges, or similar measures); and (3) the use of automated processes, devices, or systems to access the site or its content.

Copyright Infringement

Finally, Snap-On asserted that O'Neil's scraping activity constituted copyright infringement.[6] Copyright infringement requires (1) ownership of a valid copyright, and (2) the copying of protectable elements of the copyrighted work. Here, because the information in the database belonged to Mitsubishi, Snap-On alleged that the scraping infringed its copyright in the "selection and arrangement" of the information.[7] O'Neil argued that Snap-On's selection and arrangement was insufficiently original to qualify for copyright protection, and that it nonetheless only copied the underlying data for which Snap-On did not own a copyright. The court nevertheless allowed the claim to proceed, holding that O'Neil had failed to sufficiently rebut the presumption of ownership of a valid copyright afforded by Snap-On's copyright registration, and that O'Neil's reproduction of the "link structure and navigational information" could be found to infringe Snap-On's copyright in selection and arrangement.[8]

Conclusion

Web scraping can be a means of creating new and innovative data collections and associated services and applications, which are useful and in demand by users. While

---

[5] *Southwest Airlines v. Farechase*, 318 F. Supp. 2d 435 (N.D. Tx., 2004).

[6] While not asserted in this case, the Digital Millennium Copyright Act (DMCA) prohibits circumvention of technological measures designed to control access to copyrighted works. Other scraping cases have allowed plaintiffs to proceed on this claim based on allegations that a scraper bypassed plaintiff's "CAPTCHA" and IP address filtering systems that were designed to block scrapers.

[7] Notably, while copyright protection for databases under U.S. law is limited, the European Union's Database Directive provides database creators with certain protections against unauthorized use of all or a substantial part of the database's contents.

[8] See also *Facebook, Inc. v. Power Ventures, Inc.,* 2009 WL 1299698 (N.D. Cal., 2009) (holding that despite the fact that Facebook did not own copyrights in the user data on Facebook pages, RAM copies that defendant's scraper software made of complete pages in violation of Facebook's terms of service infringed Facebook's copyright in its selection and arrangement of elements on the page).

Continued on page 3...

Ohio District Court Allows Database "Scraping" Case . . .

Continued from page 2...

only a summary judgment case and therefore not a final ruling on any matter, the *Snap-On* case is a timely reminder of the legal issues that can arise with automated scraping, crawling, and data-mining activities. Technology and data service providers should give consideration to the principles discussed above in planning and implementing their businesses. If you or your company would like further information on these issues, please contact any member of Wilson Sonsini Goodrich & Rosati's technology transactions practice or intellectual property litigation department.

WSGR

Wilson Sonsini Goodrich & Rosati

PROFESSIONAL CORPORATION

650 Page Mill Road
Palo Alto, CA 94304-1050
Tel: (650) 493-9300 Fax: (650) 493-6811
email: wsgr_resource@wsgr.com

www.wsgr.com