Bloomberg Law Reports®

November 9, 2011

Technology Law

Computer & Internet Crimes

Unauthorized Access

New Age Technology: Brazilian and U.S. Courts "Scraping" the Surface of Legal Boundaries of Internet Use

Norris McLaughlin & Marcus, P.A.
Attorneys At Law

OPICE BLUM
Advogados Associados

Contributed by Fernando M. Pinguelo, Norris, McLaughlin & Marcus, P.A.; Renato Opice Blum and Kristen M. Welsh, Schiffman, Abraham, Kaufman & Ritter, P.C.

The Internet has afforded anyone, anywhere, a wealth of information at one's fingertips. Within the current and ever-expanding age of technology, Brazilian- and U.S.-based courts continue to draw legal boundaries within a seemingly boundless cyberspace. The boundlessness of the Internet, and its related technologies, transcends geographical limits and poses worldwide issues of regulation.

One such technology, which has caught the attention of businesses and resulted in significant legal battles, is "scraping" - a computer software technique that extracts publicly available information from websites. While in and of itself, "scraping" may not be unlawful, courts in Brazil and the U.S. have begun to carve out permissible and impermissible uses of this technology.

Brazilian Scraping Lawsuit

A recent court opinion of first impression in São Paulo, Brazil, gives newfound meaning to ownership rights of information available on the Internet. The Brazilian court's opinion in *Curriculum Tecnologia Ltda. v. Catho Online S/C Ltda., et al*, examines claims of unfair competition and violation of copyright rules, as applicable to the Internet. The plaintiff, Curriculum Tecnologia Ltda. ("Curriculum"), and defendant, Catho Online S/C Ltda. ("Catho"), are employment recruitment companies, operating solely through the Internet. Thousands of individuals seeking employment use the services of these companies by posting their resumes on the respective websites. In turn, employers seeking to hire review thousands of potential candidates to fill their open positions. In fact, Curriculum is the largest employment website in Brazil, providing a meeting place for over 6 million registered applicants and 100 thousand user companies. These services allow for a faster and easier connection to the open job market.

In February 2002, developers at Curriculum noticed an unusual increase in activity on their company's website. While, generally, Curriculum's customers search approximately 500 resumes per day on its website, developers became suspicious when one particular user registered over 63,000 searches in one day. Upon further investigation, Curriculum technicians blocked the particular account and tracked its origin back to a computer at Catho, the defendant competitor. As a result of its investigation and findings, Curriculum filed suit against Catho alleging various business-related claims.

As the lawsuit proceeded in the normal course, fact gathering efforts revealed flagrant and deceptive practices by Catho to illegally, in violation of Brazilian law, acquire information from Curriculum's website. In short, Catho developed a program that enabled it to copy *en mass* Curriculum's website information database through which it could access resumes from Curriculum's website. Once Catho gained access to the resume information, it used it for its own commercial purposes. The purpose behind Catho's efforts was to increase its own potential employee base in order to offer a wider range to online employment recruiters. Catho acquired hundreds of thousands of resumes from its competitors through the use of these and related methods. Indeed, Curriculum was not the only competitor to bring suit against Catho for these practices, as several other victims of this Internet hacking scheme brought separate actions against Catho.

To appreciate the breach of security and the value of the acquired information, one must understand the function of the employment recruitment market in Brazil within which these parties operate. Both parties operate primarily as online employment search engines. Individuals who seek employment and employers who seek skilled individuals, use the services of these recruitment companies by paying fees which permit the posting of resumes and job advertisements, allowing for searches of both to be performed. These web-based services offer various levels of fee-based access to these postings and search capabilities, which in turn generate revenue for these companies.

Curriculum's website provides its users with instructions and several menus that allow them to browse its webpage efficiently and effectively. Curriculum does not provide every user with access to its resume bank. Instead, the website uses filters that permit only certain clientele with particular fee-based account settings to access this information.

Catho used hacking programs to breach these security devices, allowing unauthorized access to resumes on Curriculum's website, spurring the lawsuit. Specifically, the programs developed by Catho allowed it to take advantage of security flaws in Curriculum's website, and gain access to the entire proprietary database - thereby transferring tens of thousands of resumes in a single clandestine night of debauchery.

After plaintiff filed suit, the parties set forth arguments before the Brazilian court in support of their respective positions. Curriculum argued it had a property ownership interest in the data, and therefore Catho engaged in unfair competition and unauthorized copying of Curriculum's information. Catho argued that the information was public, access to the website was open and unrestricted, and therefore the information was not afforded legal protection.

In sustaining a lower court's previous finding of damages, Judge Luiz Mario Galbetti of 33 Civil Court of São Paulo found that Catho engaged in unfair competition by breaching Curriculum's internal computer systems and illegally acquiring thousands of resumes posted therein. The court held that the transmission and expansion of Catho's own database through this illegal acquisition served to increase its market visibility with direct effects on the profits obtained by Catho. Relying on notions of unfair enrichment, abuse of rights, and unpredictability, the court awarded damages in the amount of R$21,828,250.00 (in Brazilian Real). In calculating damages, the court considered the amount charged by Catho per month for posting a resume on its website, R$50.00, multiplied by the 436,595 resumes it illegally acquired. With interest and additional penalties this R$21,828,250.00 resulted in an award of R$63 million in damages, or approximately $42 Million USD.

U.S. Scraping Lawsuits

Similarly, U.S.-based courts have addressed the legal boundaries of extracting information from public websites. In *EF Cultural Travel v. Zefer Corp.*, 318 F.3d 58 (1st Cir.2003), the U.S. Court of Appeals for the First Circuit issued a preliminary injunction pursuant to the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. 1030, to prohibit the use of a "scraper" software program that defendants used to collect pricing information from the plaintiff/competitor's website. Zefer Corp. ("Zefer") sought review of the injunction, implemented in a prior hearing with co-defendant Explorica, Inc. ("Explorica"). *See EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001).

EF and Explorica are competitors in the student travel business, operating websites that permit their respective visitors to explore various vacation packages. To gain a competitive edge, Explorica hired Zefer to build a program that would allow Explorica to "scrape" the prices from EF's website and download them into an Excel spreadsheet. After accessing EF's vacation package pricing, Explorica tailored its own costs, purposefully undercutting EF on an average of 5%. EF stumbled upon the "scraping" scheme as a result of discovery in an unrelated, state court lawsuit involving Explorica. As a result, EF filed suit in federal court, seeking an injunction on the grounds that the "scraping" violated both federal copyright laws and various provisions of the CFAA.

The underlying issue in the case was whether the use of the scraper program exceeded "authorized access," in violation of federal law. The relevant CFAA provision examined by the court provides:

> Whoever. . . knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period . . . shall be punished as provided in subsection (c) of this section.

While the CFAA defines "exceeds authorized access" as "to access a computer without authorization and to use such access to obtain or alter information in the computer that the accesseer is not entitled so to obtain or alter," the court in *EF Cultural Travel* provided analysis of the term "authorization." The trial court held that authorization could be determined both explicitly, for example through a direct statement restricting access, or

implicitly. In defining the implicit prong, the trial court relied upon a "reasonable expectations" test. Even though the appeals court agreed that authorization can be both explicit and implicit, it rejected application of the reasonable expectations test used by the trial court. Instead, the appeals court determined that "public website provider[s] can easily spell out explicitly what is forbidden and consonantly, that nothing justifies putting users at the mercy of a highly imprecise, litigation-spawning standard like 'reasonable expectations.'"

As a result, the appeals court determined that a clear manifestation of the company's intent that no information be collected from its website was necessary in order to show "lack of authorization," such as an explicit statement on the webpage restricting access. Or, to put it more bluntly, "[i]f EF wants to ban scrapers, let it say so on the webpage or a link clearly marked as containing restrictions." Nonetheless, this federal appeals court decision did not eliminate the concept of implicit authorization, as it may suffice in other circumstances. However, the decision highlighted that a plaintiff must demonstrate unambiguously that authorization was prohibited.

The *EF Cultural Travel* decision promulgates the theory that the right to control access implicates a right to prevent or obtain legal remedies for any unauthorized access. As demonstrated in *EF Cultural Travel*, authorization may be established both implicitly and explicitly. Another method of disclosing a lack of authorization may be through the creation of technological barriers, such as encryption of particular information. Under this regime, after the initial encounter, a third party must either obtain permission or take unusual steps to circumvent the technological barrier. Lastly, database owners may also establish use authorization conditions through contractual terms.

Whatever the means of establishing authorization, or the lack thereof, it is apparent that a reasonable effort to protect is a precondition to maintaining this legal right.[1] It is recognized, however, that the mere posting of information on a public domain, such as the Internet, does not in and of itself extinguish a protectable right to that information. This presumption is also echoed in case law analyzing the misappropriation of trade secrets.

For example, in *Barnett, Inc. v. Shidler*, 338 F.3d 1125 (10th Cir. 2003), the court examined whether former employees misappropriated a trade secret by implementing the Infant Swimming Research program ("ISR"), which was designed by plaintiff as a scientific, behavioral approach to pediatric drowning prevention. In finding the ISR program was not a trade secret, the trial court noted "[plaintiff] allowed its program to become part of the public domain before seeking protection...," referring to various published books explaining the ISR method. In reversing this finding, the appeals court highlighted the decision in *Rivendell Forest Prods., Ltd. v. Georgia-Pacific Corp.*, 28 F.3d 1042, 1045 (10th Cir.1994) in which the court found that "a trade secret can exist in combination of characteristics, each of which, considered separately, is in the public domain, but, taken together, may yield a competitive advantage that results in a protectable trade secret," solidifying the argument that information may be a trade secret notwithstanding the fact that some of its components are well known. *See also Syncsort v. Innovative Routines*, No. 04-CV-03623, 2011 BL 213594 (D.N.J. Aug. 18, 2011) (federal district court of New Jersey examining the existence of a trade secret in light of its brief publishing on the internet). While case law involving scraping requires some form of notification as to non-authorization, this line of reasoning quashes any argument that information posted on the Internet should not enjoy legal protection simply because of its public nature.

A court must determine the underlying intent of the scraper because the legality of extracting data from a website often centers on the underlying intent in copying.[2] The copying of information for any purpose deemed a "fair use" may therefore not be actionable. As evidenced by both *EF Cultural Travel* and *Curriculum*, this key element is what often implicates legal remedies.

Lessons Learned

Easy access to information afforded by the Internet has created a global culture that often accepts the free use (and abuse) of information. This often results in blurred lines between public and private property, especially for those who conduct business through the Internet.

Therefore, unless a database is composed of content independently entitled to protection, for example through copyright or trade secret law, database owners must rely upon a patchwork of available legal remedies. Database owners may seek protection under unfair trade statutes or under common law theories such as misappropriation. Contractual restrictions also offer protection, but such a remedy requires privity of contract. Moreover, while a claim for trespass may also be a feasible option, most courts require a showing of actual injury. Lastly, and certainly not exclusively, protection under the CFAA may be warranted. While each option has its own nuances, courts are setting down the foundation of protection in response to the legalities of the Internet age. Therefore, while the potential remedies available to database owners under U.S. law tend to be narrow, it is no doubt only the beginning.

Regardless of the underlying legal principal asserted against an illegal scraper, liability attaches on a case by case basis depending upon the type of access obtained by the scraper, the amount of information accessed and copied, the degree to which the access adversely affects the Web site owner's system and the types and manner of prohibitions on such conduct.

The significant monetary award issued by the São Paulo court underscores the value that information has to a company and its survival. The decision also serves as a warning to billions of Internet users globally, as the calculation of damages serves not only to punish the wrongdoer but also to deter the illegal activity in and of itself.

These decisions evidence a fairly new attempt by courts to address the legal issues posed by the Internet. While the approach is not yet uniform, there are obvious efforts by courts to protect proprietary information on the Internet from uses that are detrimental to the owners of such sites.

Fernando M. Pinguelo, a Partner at Norris, McLaughlin & Marcus, P.A. and co-Chair of the Response to Electronic Discovery & Information Group at the firm, is a U.S.-based trial lawyer who devotes his practice to complex business lawsuits with an emphasis on how technology impacts lawsuits. Mr. Pinguelo founded and contributes to the ABA Journal award-winning blog, eLessons Learned - Where Law, Technology, & Human Error Collide (www.eLLblog.com). To learn more about Mr. Pinguelo, visit www.NYLocalLaw.com or email him at info@NYLocalLaw.com.

Renato Opice Blum, CEO of Opice Blum Advogados Associados in São Paulo, Brazil, is a Brazil-based attorney and economist, who established one of the first leading technology-based law firms. Mr. Blum is the Coordinator of the MBA course in Information Technology Law at São Paulo State Law School and a distinguished professor at Fundação Getúlio Vargas, among other universities. Mr. Blum is co-author of the book, Internet and Electronic Law. To learn more about Mr. Blum, visit http://www.opiceblum.com.br/lang-en/01_profissionais_dadosRes.php?ID_CUREQUIPE=138578 or email him at renato@opiceblum.com.br.

Kristen M. Welsh is a U.S.-based litigation Associate at Schiffman, Abraham, Kaufman & Ritter, P.C. and focuses her practice on business and employment law matters. Ms. Welsh may be reached at KWelsh@sakr-law.com.

[1] This rule of thumb is also applied in cases analyzing the misappropriation of trade secrets. *See Barnett, Inc. v. Shidler,* 338 F.3d 1125 (10th Cir. 2003).

[2] Various fair uses have been identified by the court. *See Nautical Solutions Mktg., Inc. v. Boats.com*, Copy. L. Rep. (CCH) ¶28, 815 (M.D. Fla. 2004) (holding that "momentary copying of open . . . public Web pages in order to extract yacht listings facts unprotected by copyright law constitutes a fair use."); *Ticketmaster Corp. v. Tickets.com, Inc.*, No. 09-CV-07654 (C.D. Cal. Mar. 7, 2003) ("Taking the temporary copy of the electronic information [from the Ticketmaster.com website database] for the limited purpose of extracting unprotected public facts leads to the conclusion that the temporary use of the electronic signals was 'fair use' and not actionable."); *see also Assessment Technologies, LLC v. WIREdata, Inc.,* 350 F.3d 640 (7th Cir. 2003).