United States Court of Appeals
For the First Circuit

No. 01-2001

EF CULTURAL TRAVEL BV, ET AL.,

Plaintiffs, Appellees,

v.

ZEFER CORPORATION,

Defendant, Appellant,

and

EXPLORICA, INC., ET AL.,

Defendants.

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

[Hon. Morris E. Lasker,* U.S. District Judge]

Before
Boudin, Chief Judge,
Torruella, Circuit Judge,
and Cyr, Senior Circuit Judge.

William A. Zucker with whom Scott J. Nathan and Gadsby Hannah, LLP were on supplemental brief for appellant.

Joan A. Lukey with whom John J. Butts and Hale and Dorr LLP were on supplemental brief for appellees.

January 28, 2003

*Of the Southern District of New York, sitting by designation.

BOUDIN, Chief Judge. Defendant Zefer Corporation ("Zefer") seeks review of a preliminary injunction prohibiting it from using a "scraper tool" to collect pricing information from the website of plaintiff EF Cultural Travel BV ("EF"). This court earlier upheld the injunction against co-defendant Explorica, Inc. ("Explorica"). EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001) ("EF I"). The validity of the injunction as applied to Zefer was not addressed because Zefer's appeal was stayed when it filed for bankruptcy, but the stay has now been lifted.

EF and Explorica are competitors in the student travel business. Explorica was started in the spring of 2000 by several former EF employees who aimed to compete in part by copying EF's prices from EF's website and setting Explorica's own prices slightly lower. EF's website permits a visitor to the site to search its tour database and view the prices for tours meeting specified criteria such as gateway (e.g., departure) cities, destination cities, and tour duration. In June 2000, Explorica hired Zefer, which provides computer-related expertise, to build a scraper tool that could "scrape" the prices from EF's website and download them into an Excel spreadsheet.

A scraper, also called a "robot" or "bot," is nothing more than a computer program that accesses information contained in a succession of webpages stored on the accessed computer. Strictly

speaking, the accessed information is not the graphical interface seen by the user but rather the HTML source code--available to anyone who views the site--that generates the graphical interface. This information is then downloaded to the user's computer. The scraper program used in this case was not designed to copy all of the information on the accessed pages (e.g., the descriptions of the tours), but rather only the price for each tour through each possible gateway city.

Zefer built a scraper tool that scraped two years of pricing data from EF's website. After receiving the pricing data from Zefer, Explorica set its own prices for the public, undercutting EF's prices an average of five percent. EF discovered Explorica's use of the scraper tool during discovery in an unrelated state-court action brought by Explorica's President against EF for back wages.

EF then sued Zefer, Explorica, and several of Explorica's employees in federal court.[1] Pertinently, EF sought a preliminary injunction on the ground that the copying violated the federal Copyright Act, 17 U.S.C. § 101 et seq. (2000), and various provisions of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030 (2000). The district court refused to grant EF summary

[1]The individual defendants are Olle Olsson, Peter Nilsson, Philip Gormley, Alexandra Bernadotte, Anders Ericksson, Deborah Johnson, and Stefan Nilsson. We refer hereafter to Explorica and the individual defendants collectively as "Explorica."

judgment on its copyright claim, but it did issue a preliminary injunction against all defendants based on one provision of the CFAA, ruling that the use of the scraper tool went beyond the "reasonable expectations" of ordinary users. The preliminary injunction states inter alia:

> [D]efendant Explorica, Inc., its officers, agents, servants, employees, successors and assigns, all persons acting in concert or participation with Explorica, Inc., and/or acting on its behalf or direction are preliminarily enjoined to . . . refrain, whether directly or indirectly, from the use of a "scraper" program, or any other similar computer tool, to access any data useable or necessary for the compilation of prices on or from the website of plaintiff EF Cultural Travel and its related entities, and/or the EF Tour Database.

The defendants appealed, but soon after briefing was completed, Zefer filed for bankruptcy and its appeal was automatically stayed. 11 U.S.C. § 362(a)(1) (2000). Explorica's appeal went forward and in EF I a panel of this court upheld the preliminary injunction against Explorica. The panel held that the use of the scraper tool exceeded the defendants' authorized access to EF's website because (according to the district court's findings for the preliminary injunction) access was facilitated by use of confidential information obtained in violation of the broad confidentiality agreement signed by EF's former employees. EF I, 274 F.3d at 582-84.

On Zefer's re-activated appeal, the question presented is whether the preliminary injunction is proper as to Zefer. We conclude that it is proper even as to Zefer, which signed no confidentiality agreement, but on relatively narrow grounds. Given the prospect of further proceedings--this appeal is merely from a preliminary injunction--it is helpful to explain where and why our own reasoning differs from that of the district court. The principal issues are legal ones as to which our review is de novo. Cablevision of Boston, Inc. v. Pub. Improvement Comm'n, 184 F.3d 88, 96 (1st Cir. 1999).

EF argues at the outset that our decision in EF I is decisive as to Zefer. But the ground we adopted there in upholding the injunction as to the other defendants was that they had apparently used confidential information to facilitate the obtaining of the EF data. Explorica was created by former EF employees, some of whom were subject to confidentiality agreements. Zefer's position in that respect is quite different than that of Explorica or former EF employees. It signed no such agreement, and its prior knowledge as to the agreement is an open question.

EF suggests that Zefer must have known that information provided to it by Explorica had been improperly obtained. This is possible but not certain, and there are no express district court findings on this issue; indeed, given the district court's much broader basis for its injunction, it had no reason to make any

detailed findings as to the role of the confidentiality agreement. What can be gleaned from the record as to Zefer's knowledge certainly does not permit us to make on appeal the finding urged by EF.

What appears to have happened is that Philip Gormley, Explorica's Chief Information Officer and EF's former Vice President of Information Strategy, e-mailed Zefer a description of how EF's website was structured and identified the information that Explorica wanted to have copied; this may have facilitated Zefer's development of the scraper tool, but there is no indication that the structural information was unavailable from perusal of the website or that Zefer would have known that it was information subject to a confidentiality agreement.

EF also claims that Gormley e-mailed Zefer the "codes" identifying in computer shorthand the names of EF's gateway and destination cities. These codes were used to direct the scraper tool to the specific pages on EF's website that contained EF's pricing information. But, again, it appears that the codes could be extracted more slowly by examining EF's webpages manually,[2] so it is far from clear that Zefer would have had to know that they

[2]As an example, the website address for an EF Tour to Paris and Geneva leaving from Boston is http://www.eftours.com/public/browse/browse_detail.asp?CTID=PTG%20V&GW=BOS. Looking closely at the website address, one can determine that the destination code for the Paris and Geneva tour is PTG, while the gateway code for Boston is BOS.

were confidential. The only information that Zefer received that was described as confidential (passwords for tour-leader access) apparently had no role in the scraper project.

EF's alternative ground for affirmance is the rationale adopted by the district court for the preliminary injunction. That court relied on its "reasonable expectations" test as a gloss on the CFAA and then applied it to the facts of this case. Although we bypassed the issue in EF I, the district court's rationale would embrace Zefer as readily as Explorica itself. But the gloss presents a pure question of law to be reviewed de novo and, on this issue, we differ with the district court.

The CFAA provision relied upon by the district court states:

> 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.

18 U.S.C. § 1030(a)(4). The statute defines "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." Id. § 1030(e)(6). The CFAA furnishes a civil remedy for individuals who suffer

damages or loss as a result of a violation of the above section. Id. § 1030(g).

At the outset, one might think that EF could have difficulty in showing an intent to defraud. But Zefer did not brief the issue on the original appeal before bankruptcy. In addition, there may be an argument that the fraud requirement should not pertain to injunctive relief. Accordingly, we bypass these matters and assume that the fraud requirement has been satisfied or is not an obstacle to the injunction.

The issue, then, is whether use of the scraper "exceed[ed] authorized access." A lack of authorization could be established by an explicit statement on the website restricting access. (Whether public policy might in turn limit certain restrictions is a separate issue.) Many webpages contain lengthy limiting conditions, including limitations on the use of scrapers.[3] However, at the time of Zefer's use of the scraper, EF had no such explicit prohibition in place, although it may well use one now.

[3]For example, the "legal notices" on one familiar website state that "you may print or download one copy of the materials or content on this site on any single computer for your personal, non-commercial use, provided you keep intact all copyright and other proprietary notices. Systematic retrieval of data or other content from this site to create or compile, directly or indirectly, a collection, compilation, database or directory without written permission from America Online is prohibited." AOL Anywhere Terms and Conditions of Use, at http://www.aol.com/copyright.html (last visited Jan. 14, 2003).

The district court thought that a lack of authorization could also be inferred from the circumstances, using "reasonable expectations" as the test; and it said that three such circumstances comprised such a warning in this case: the copyright notice on EF's homepage with a link directing users to contact the company with questions; EF's provision to Zefer of confidential information obtained in breach of the employee confidentiality agreements; and the fact that the website was configured to allow ordinary visitors to the site to view only one page at a time.

We agree with the district court that lack of authorization may be implicit, rather than explicit. After all, password protection itself normally limits authorization by implication (and technology), even without express terms. But we think that in general a reasonable expectations test is not the proper gloss on subsection (a)(4) and we reject it. However useful a reasonable expectations test might be in other contexts where there may be a common understanding underpinning the notion, cf. Terry v. Ohio, 392 U.S. 1, 9 (1968) (Fourth Amendment), its use in this context is neither prescribed by the statute nor prudentially sound.

Our basis for this view is not, as some have urged, that there is a "presumption" of open access to Internet information. The CFAA, after all, is primarily a statute imposing limits on access and enhancing control by information providers. Instead, we

think that the public website provider 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." If EF wants to ban scrapers, let it say so on the webpage or a link clearly marked as containing restrictions.

This case itself illustrates the flaws in the "reasonable expectations" standard. Why should the copyright symbol, which arguably does not protect the substantive information anyway, Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 344-45 (1991), or the provision of page-by-page access for that matter, be taken to suggest that downloading information at higher speed is forbidden. EF could easily include--indeed, by now probably has included--a sentence on its home page or in its terms of use stating that "no scrapers may be used," giving fair warning and avoiding time-consuming litigation about its private, albeit "reasonable," intentions.

Needless to say, Zefer can have been in no doubt that EF would dislike the use of the scraper to construct a database for Explorica to undercut EF's prices; but EF would equally have disliked the compilation of such a database manually without the use of a scraper tool. EF did not purport to exclude competitors from looking at its website and any such limitation would raise serious public policy concerns. Cf. Food Lion, Inc. v. Capital Cities/ABC,

Inc., 194 F.3d 505, 516-18 (4th Cir. 1999); Desnick v. Am. Broad. Cos., 44 F.3d 1345, 1351 (7th Cir. 1995).

Although we conclude that the district court's rationale does not support an independent preliminary injunction against Zefer, there is no apparent reason to vacate the present injunction "as against Zefer." Despite being a party to the case, Zefer is not named in the ordering language of the injunction; it is merely precluded, like anyone else with notice, from acting in concert with, on behalf of, or at the direction of Explorica to use the scraper to access EF's information.

Under the applicable rules and case law, an injunction properly issued against a named party means that anyone else with notice is precluded from acting to assist the enjoined party from violating the decree or from doing so on behalf of that party. See Fed. R. Civ. P. 65(d); G. & C. Merriam Co. v. Webster Dictionary Co., 639 F.2d 29, 34-35 (1st Cir. 1980). There is no reason why Zefer should be freer than any other third party who was never in this litigation to assist EF to violate the injunction against it or to do so on EF's behalf or at its direction. As we read the injunction, that is all that is forbidden.

It may still be of practical importance to Zefer to have clarified the limited basis on which we uphold the injunction. And nothing we have said would prevent EF, if it matters in continued litigation, from seeking to show that Zefer did use confidential

information, aware that it was being supplied in violation of agreements made by former EF employees. It is also of some use for future litigation among other litigants in this circuit to indicate that, with rare exceptions, public website providers ought to say just what non-password protected access they purport to forbid.

Lastly, Zefer has alleged that the First Amendment would be offended if the statute were construed to forbid generally the use of scrapers to collect otherwise available information where there was no intent to defraud or harm the target website. Here, the preliminary injunction is premised on EF's misuse of confidential information and Zefer thus far is constrained only in helping a tentatively-identified wrongdoer in exploiting that confidential information. Cf. San Francisco Arts & Athletics, Inc. v. U.S. Olympic Comm., 483 U.S. 522, 541 (1987). None of Zefer's arguments address this narrowed constraint or suggest to us that it is constitutionally doubtful.

The preliminary injunction is affirmed on the limited basis set forth above and as construed by this court. Each side shall bear its own costs on this appeal.