

274 F.3d 577

United States Court of Appeals,
First Circuit.

EF CULTURAL TRAVEL BV, EF Cultural
Tours BV, EF Institute for Cultural Exchange,
Inc., EF Cultural Services BV, and Go Ahead
Vacations, Inc., Plaintiffs, Appellees,
v.

EXPLORICA, INC., Olle Olsson, Peter Nilsson,
Philip Gormley, Alexandra Bernadotte, Anders
Eriksson, Deborah Johnson, and Stefan Nilsson,
Defendants, Appellants.

Decided Dec. 17, 2001.

Before BOUDIN, Chief Judge, COFFIN, Senior
Circuit Judge, and LYNCH, Circuit Judge.

COFFIN, Senior Circuit Judge.

Appellant Explorica, Inc. (“Explorica”) and several of its employees challenge a preliminary injunction issued against them for alleged violations of the Computer Fraud and Abuse Act (“CFAA”), 18 U.S.C. § 1030.¹ We affirm the district court’s conclusion that appellees will likely succeed on the merits of their CFAA claim, but rest on a narrower basis than the court below.

I. Background

Explorica was formed in 2000 to compete in the field of global tours for high school students. Several of Explorica’s employees formerly were employed by appellee EF, which has been in business for more than thirty-five years. EF and

¹ The individual defendants-appellants are Olle Olsson, Peter Nilsson, Philip Gormley, Alexandra Bernadotte, Anders Eriksson, Deborah Johnson, and Stefan Nilsson. They are all former employees of plaintiffs-appellees, EF Cultural Tours BV, EF Institute for Cultural Exchange, Inc. (“EFICE”), EF Cultural Services BV, and Go Ahead Vacations, Inc. The appellees are collectively referred to as “EF.”

its partners and subsidiaries make up the world’s largest private student travel organization.

Shortly after the individual defendants left EF in the beginning of 2000, Explorica began competing in the teenage tour market. The company’s vice president (and former vice president of information strategy at EF), Philip Gormley, envisioned that Explorica could gain a substantial advantage over all other student tour companies, and especially EF, by undercutting EF’s already competitive prices on student tours. Gormley considered several ways to obtain and utilize EF’s prices: by manually keying in the information from EF’s brochures and other printed materials; by using a scanner to record that same information; or, by manually searching for each tour offered through EF’s website. Ultimately, however, Gormley engaged Zefer, Explorica’s Internet consultant, to design a computer program called a “scraper” to glean all of the necessary information from EF’s website. Zefer designed the program in three days.

The scraper has been likened to a “robot,” a tool that is extensively used on the Internet. Robots are used to gather information for countless purposes, ranging from compiling results for search engines such as Yahoo! to filtering for inappropriate content. The widespread deployment of robots enables global Internet users to find comprehensive information quickly and almost effortlessly.

Like a robot, the scraper sought information through the Internet. Unlike other robots, however, the scraper focused solely on EF’s website, using information that other robots would not have. Specifically, Zefer utilized tour codes whose significance was not readily understandable to the public. With the tour codes, the scraper accessed EF’s website repeatedly and easily obtained pricing information for those specific tours. The scraper sent more than 30,000 inquiries to EF’s website and recorded the pricing information into a spreadsheet.

Zefer ran the scraper program twice, first to retrieve the 2000 tour prices and then the 2001 prices. All told, the scraper downloaded 60,000 lines of data, the equivalent of eight telephone directories of information. Once Zefer “scraped” all of the prices, it sent a spreadsheet containing EF’s pricing information to Explorica, which then systematically undercut EF’s prices. Explorica thereafter printed its own brochures and began competing in EF’s tour market.

The development and use of the scraper came to light about a year and a half later during state-court litigation regarding appellant Olsson’s departure from appellee EFICE. EF then filed this action, alleging violations of the CFAA; the Copyright Act of 1976, 17 U.S.C. § 101; the Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. § 1961; and various related state laws. It sought a preliminary injunction barring Explorica and Zefer from using the scraper program and demanded the return of all materials generated through use of the scraper.

On May 30, 2001, the district court granted a preliminary injunction against Explorica based on the CFAA, which criminally and civilly prohibits certain access to computers. See 18 U.S.C. § 1030(a)(4). The court found that EF would likely prove that Explorica violated the CFAA when it used EF’s website in a manner outside the “reasonable expectations” of both EF and its ordinary users. The court also concluded that EF could show that it suffered a loss, as required by the statute, consisting of reduced business, harm to its goodwill, and the cost of diagnostic measures it incurred to evaluate possible harm to EF’s systems, although it could not show that Explorica’s actions physically damaged its computers. In a supplemental opinion the district court further articulated its “reasonable expectations” standard and explained that copyright, contractual and technical restraints sufficiently notified Explorica that its use of a scraper would be unauthorized and thus would violate the CFAA.

The district court first relied on EF’s use of a copyright symbol on one of the pages of its website and a link directing users with questions

to contact the company, finding that “such a clear statement should have dispelled any notion a reasonable person may have had that the ‘presumption of open access’ applied to information on EF’s website.” The court next found that the manner by which Explorica accessed EF’s website likely violated a confidentiality agreement between appellant Gormley and EF, because Gormley provided to Zefer technical instructions concerning the creation of the scraper. Finally, the district court noted without elaboration that the scraper bypassed technical restrictions embedded in the website to acquire the information. The court therefore let stand its earlier decision granting the preliminary injunction. Appellants contend that the district court erred in taking too narrow a view of what is authorized under the CFAA and similarly mistook the reach of the confidentiality agreement. Appellants also argue that the district court erred in finding that appellees suffered a “loss,” as defined by the CFAA, and that the preliminary injunction violates the First Amendment.

II. Standard of Review

A district court may issue a preliminary injunction only upon considering (1) the likelihood of success on the merits; (2) the potential for irreparable harm if the injunction is denied; (3) the balance of relevant impositions ...; and (4) the effect (if any) of the court’s ruling on the public interest. Appellants challenge only the district court’s finding that appellees are likely to succeed on the merits, and we thus confine our review to that factor. [. . .]

III. The Computer Fraud and Abuse Act

Although appellees alleged violations of three provisions of the CFAA, the district court found that they were likely to succeed only under section 1030(a)(4). That section 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... shall be punished.

18 U.S.C. § 1030(a)(4).⁸

Appellees allege that the appellants knowingly and with intent to defraud accessed the server hosting EF's website more than 30,000 times to obtain proprietary pricing and tour information, and confidential information about appellees' technical abilities. At the heart of the parties' dispute is whether appellants' actions either were "without authorization" or "exceed[ed] authorized access" as defined by the CFAA. We conclude that because of the broad confidentiality agreement appellants' actions "exceed[ed] authorized access," and so we do not reach the more general arguments made about statutory meaning, including whether use of a scraper alone renders access unauthorized.¹⁰

A. "Exceeds authorized access"

Congress defined "exceeds authorized access," as accessing "a computer with authorization and [using] such access to obtain or alter information

⁸ Although the CFAA is primarily a criminal statute, under § 1030(g), "any person who suffers damage or loss ... may maintain a civil action ... for compensatory damages and injunctive relief or other equitable relief."

¹⁰ Congress did not define the phrase "without authorization," perhaps assuming that the words speak for themselves. The meaning, however, has proven to be elusive. The district court applied what it termed the "default rule" that conduct is without authorization only if it is not "in line with the reasonable expectations" of the website owner and its users. Appellants argue that this is an overly broad reading that restricts access and is at odds with the Internet's intended purpose of providing the "open and free exchange of information." They urge us to adopt instead the Second Circuit's reasoning that computer use is "without authorization" only if the use is not "in any way related to [its] intended function," *United States v. Morris*, 928 F.2d 504, 510 (2d Cir.1991). Appellees contend that the result would be the same under either test, but we need not resolve this dispute because we affirm the court's ruling based on the "exceeds authorized access" prong of § 1030(a)(4).

in the computer that the accessor is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). EF is likely to prove such excessive access based on the confidentiality agreement between Gormley and EF. Pertinently, that agreement provides:

Employee agrees to maintain in strict confidence and not to disclose to any third party, either orally or in writing, any Confidential or Proprietary Information ... and never to at any time (i) directly or indirectly publish, disseminate or otherwise disclose, deliver or make available to anybody any Confidential or Proprietary Information or (ii) use such Confidential or [P]roprietary Information for Employee's own benefit or for the benefit of any other person or business entity other than EF.

* * *

As used in this Agreement, the term "Confidential or Proprietary Information" means (a) any trade or business secrets or confidential information of EF, whether or not reduced to writing ...; (b) any technical, business, or financial information, the use or disclosure of which might reasonably be construed to be contrary to the interests of EF.

...

The record contains at least two communications from Gormley to Zefer seeming to rely on information about EF to which he was privy only because of his employment there. First, in an email to Zefer employee Joseph Alt exploring the use of a scraper, Gormley wrote: "[m]ight one of the team be able to write a program to automatically extract prices ... ? I could work with him/her on the specification." Gormley also sent the following email to Zefer employee John Hawley:

Here is a link to the page where you can grab EF's prices. There are two important drop down menus on the right.... With the lowest one you select one of about 150 tours. * * * You then select your origin gateway from a list of about 100 domestic

gateways (middle drop down menu). When you select your origin gateway a page with a couple of tables comes up. One table has 1999- 2000 prices and the other has 2000-2001 prices. * * * On a high speed connection it is possible to move quickly from one price table to the next by hitting backspace and then the down arrow.

This documentary evidence points to Gormley's heavy involvement in the conception of the scraper program. Furthermore, the voluminous spreadsheet containing all of the scraped information includes the tour codes, which EF claims are proprietary information. Each page of the spreadsheet produced by Zefer includes the tour and gateway codes, the date of travel, and the price for the tour. An uninformed reader would regard the tour codes as nothing but gibberish.¹¹ Although the codes can be correlated to the actual tours and destination points, the codes standing alone need to be "translated" to be meaningful.

Explorica argues that none of the information Gormley provided Zefer was confidential and that the confidentiality agreement therefore is irrelevant. The case on which they rely, *Lanier Professional Services, Inc. v. Ricci*, 192 F.3d 1, 5 (1st Cir.1999), focused almost exclusively on an employee's non-compete agreement. The opinion mentioned in passing that there was no actionable misuse of confidential information because the only evidence that the employee had taken protected information was a "practically worthless" affidavit from the employee's successor. *Id.* at 5.

Here, on the other hand, there is ample evidence that Gormley provided Explorica proprietary information about the structure of the website and the tour codes. To be sure, gathering manually the various codes through repeated searching and deciphering of the URLs theoretically may be possible. Practically speaking,

¹¹ An example of the website address including the tour information is <http://www.eftours.com/tours/PriceResult.asp? Gate=GTF & TourID=LPM>. In this address, the proprietary codes are "GTF" and "LPM."

however, if proven, Explorica's wholesale use of EF's travel codes to facilitate gathering EF's prices from its website reeks of use—and, indeed, abuse—of proprietary information that goes beyond any authorized use of EF's website.

Gormley voluntarily entered a broad confidentiality agreement prohibiting his disclosure of any information "which might reasonably be construed to be contrary to the interests of EF." Appellants would face an uphill battle trying to argue that it was not against EF's interests for appellants to use the tour codes to mine EF's pricing data. If EF's allegations are proven, it will likely prove that whatever authorization Explorica had to navigate around EF's site (even in a competitive vein), it exceeded that authorization by providing proprietary information and know-how to Zefer to create the scraper.¹⁶ Accordingly, the district court's finding that Explorica likely violated the CFAA was not clearly erroneous.

B. Damage or Loss under section 1030(g)

[...]

IV. Conclusion

For the foregoing reasons, we agree with the district court that appellees will likely succeed on the merits of their CFAA claim under 18 U.S.C. § 1030(a)(4). Accordingly, the preliminary injunction was properly ordered.

Affirmed.

¹⁶ . . . [W]e express no opinion on the district court's ruling that EF's copyright notice served as a "clear statement [that] should have dispelled any notion a reasonable person may have had the 'presumption of open access'" to EF's website.