United States Court of Appeals
For the First Circuit

No. 01-2000

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.

APPEAL FROM THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF MASSACHUSETTS

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

Before

Boudin, Chief Judge,
Coffin, Senior Circuit Judge,
and Lynch, Circuit Judge.

Anthony M. Feeherry, with whom James W. Nagle, R. David Hosp, and Goodwin Proctor LLP were on brief, for appellants.

Nathaniel H. Akerman, with whom Seyfarth Shaw was on brief, for appellees.

December 17, 2001

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 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

[1] The individual defendants-appellants are Olle Olsson, Peter Nilsson, Philip Gormley, Alexandra Bernadotte, Anders Erikkson, 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."

The injunction was also issued against a second company, Zefer Corporation ("Zefer"), which also appealed. After briefing was completed, Zefer filed for bankruptcy. We granted a joint motion to sever Zefer's appeal, which has been stayed.

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.[2]

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

[2] John Hawley, one of Zefer's senior technical associates, explained the technical progression of the scraper in an affidavit:

> [a.] Open an Excel spreadsheet. The spreadsheet initially contains EFTours gateway and destination city codes, which are available on the EFTours web site.
>
> [b.] Identify the first gateway and destination city codes [on the] Excel spreadsheet.
>
> [c.] Create a [website address] request for the EFTours tour prices page based on a combination of gateway and destination city. Example: show me all the prices for a London trip leaving JFK.
>
> [d.] View the requested web page which is retained in the random access memory of the requesting computer in the form of HTML [computer language] code. * * *
>
> [e.] Search the HTML for the tour prices for each season, year, etc.
>
> [f.] Store the prices into the Excel spreadsheet.
>
> [g.] Identify the next gateway and city codes in the spreadsheet.
>
> [8.] Repeat steps 3-7 for all gateway and destination city combinations.

telephone directories of information.[3] 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.[4] 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

[3] Appellants dispute the relevance of the size of the printed data, arguing that 60,000 printed lines, while voluminous on paper, is not a large amount of data for a computer to store. This is a distinction without a difference. The fact is that appellants utilized the scraper program to download EF's pricing data. In June 2000, EF's website listed 154,293 prices for various tours.

[4] Explorica later varied its prices slightly to mask its across-the-board discount of EF’s prices.

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[5] 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,[6] finding that "such

[5] Zefer, Explorica's consultant, had objected to the initial decision on the ground that it could face liability under the preliminary injunction even though it had not had an opportunity to respond to EF's preliminary injunction motion. The district court allowed all of the parties to submit supplemental briefs and issued a further decision on July 2, 2001.

[6] The notice stated in full:

> Copyright © 2000 EF Cultural Travel BV

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

EF Educational Tours is a member of the EF group of companies.
Questions? Please contact us.

denied; (3) the balance of relevant impositions . . . ; and (4) the effect (if any) of the court's ruling on the public interest." Ross-Simons of Warwick, Inc. v. Baccarat, Inc., 102 F.3d 12, 15 (1st Cir. 1996). 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. As in any other appeal, we review the merits of a preliminary injunction depending on the issue under consideration. "Generally speaking, pure issues of law (e.g., the construction of a statute) are reviewed de novo, findings of fact for clear error, and 'judgment calls' with considerable deference. . . ." Langlois v. Abington Hous. Auth., 207 F.3d 43, 47 (1st Cir. 2000). Each of these is applicable here, where the district court's judgment relied on both its analysis of the CFAA and its assessment of the voluminous documentary evidence.

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).[7] 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

[7] Appellees have not challenged the district court's finding that they were unlikely to succeed on claims brought under 18 U.S.C. §§ 1030(5)(C) and(6)(A).

> 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.[9] 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

[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."

[9] At oral argument, appellants contended that they had no "intent to defraud" as defined by the CFAA. That argument was not raised in the briefs and thus has been waived. See Garcia-Ayala v. Parenterals, Inc., 212 F.3d 638, 645 (1st Cir. 2000) (failure to brief an argument constitutes waiver despite attempt to raise the argument at oral argument). Likewise, at oral argument Explorica attempted to adopt appellant Zefer's argument that the preliminary injunction violates the First Amendment. The lateness of Explorica's attempt renders it fruitless. See id.

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 in the computer that the accesser 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

[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).

> 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.[12] 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

[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."

[12] The Agreement provides that confidential information does not include anything that "is or becomes generally known within EF's industry."

structure of the website and the tour codes. To be sure, gathering manually the various codes through repeated searching and deciphering of the URLs[13] theoretically may be possible. Practically speaking, 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.[14]

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."[15] 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. See Anthony's Pier Four,

[13] URL is the acronym for "uniform resource locator," the technical name for the web address typed in by an Internet user. For example, EF's URL is http://www.eftours.com.

[14] Among the several emails in the record is one from Zefer employee Joseph Alt to the Explorica "team" at Zefer:

> Below is the information needed to log into EF's site as a tour leader. Please use this to gather competitor information from both a business and experience design perspective. We may also be able to glean knowledge of their technical abilities. As with all of our information, this is extremely confidential. Please do not share it with anyone.

[15] Ironically, appellant Olsson countersigned Gormley's confidentiality agreement as the representative of EF.

Inc. v. HBC Assoc., 411 Mass. 451, 471, 583 N.E.2d 806, 820 (1991) (imposing a duty of good faith and fair dealing in all contracts under Massachusetts law). 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.

[16] EF also claims that Explorica skirted the website's technical restraints. To learn about a specific tour, a user must navigate through several different web pages by "clicking" on various drop-down menus and choosing the desired departure location, date, tour destination, tour length, and price range. The district court found that the scraper circumvented the technical restraints by operating at a warp speed that the website was not normally intended to accommodate. We need not reach the argument that this alone was a violation of the CFAA, however, because the apparent transfer of information in violation of the Confidentiality Agreement furnishes a sufficient basis for injunctive relief.

Likewise, we 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.

B. Damage or Loss under section 1030(g)

Appellants also challenge the district court's finding that the appellees would likely prove they met the CFAA's "damage or loss" requirements. Under the CFAA, EF may maintain a private cause of action if it suffered "damage or loss." 18 U.S.C. § 1030(g). "Damage" is defined as "any impairment to the integrity or availability of data, a program, a system, or information that . . . causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals . . . . " 18 U.S.C. § 1030(e)(8). "Loss" is not defined.

The district court held that although EF could not show any "damage" it would likely be able to show "loss" under the statute. It reasoned that a general understanding of the word "loss" would fairly encompass a loss of business, goodwill, and the cost of diagnostic measures that EF took after it learned of Explorica's access to its website.[17] Appellants respond that such diagnostic measures cannot be included in the $5,000 threshold because their actions neither caused any physical damage nor placed any stress on EF's website.

[17] It is undisputed that appellees paid $20,944.92 to assess whether their website had been compromised. Appellees also claim costs exceeding $40,000 that they will incur to "remedy and secure their website and computer." We need not consider whether these expenses constitute loss because the initial $20,944.92 greatly exceeds the threshold.

Few courts have endeavored to resolve the contours of damage and loss under the CFAA. See, e.g., Shaw v. Toshiba Am. Info. Sys., 91 F. Supp. 2d 926 (E.D. Tex. 1999) (noting the paucity of decisions construing the Act). Two district courts that have addressed the issue have found that expenses such as those borne by EF do fall under the statute. In Shurgard Storage Center v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121 (W.D. Wa. 2000), the district court found that the need to assess whether a defendant's actions compromised the plaintiff's computers was compensable under the CFAA because the computer's integrity was called into question. The court based its finding on the legislative history of the 1996 amendments to the CFAA:

> The 1994 Amendment required both "damage" and "loss," but it is not always clear what constitutes "damage." For example, intruders often alter existing log-on programs so that user passwords are copied to a file which the hackers can retrieve later. After retrieving the newly created password file, the intruder restores the altered log-on file to its original condition. Arguably, in such a situation, neither the computer nor its information is damaged. Nonetheless, this conduct allows the intruder to accumulate valid user passwords to the system, requires all system users to change their passwords, and requires the system administrator to devote resources to re-securing the system. Thus, although there is arguably no "damage," the victim does suffer "loss." If the loss to the victim meets the required monetary threshold, the conduct should be criminal, and the victim should be entitled to relief.

S. Rep. No. 104-357, at 11 (1996) (quoted in Shurgard, 119 F. Supp. 2d at 1126). Another district court held that this legislative history makes "clear that Congress intended the term 'loss' to target remedial expenses borne by victims that could not properly be considered direct damage caused by a computer hacker." In re Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497, 521 (S.D.N.Y. 2001).

We agree with this construction of the CFAA. In the absence of a statutory definition for "loss," we apply the well-known rule of assigning undefined words their normal, everyday meaning. See Inmates of Suffolk Cty. Jail v. Rouse, 129 F.3d 649, 653-54 (1st Cir. 1997). The word "loss" means "detriment, disadvantage, or deprivation from failure to keep, have or get." The Random House Dictionary of the English Language 1137 (2d ed. 1983). Appellees unquestionably suffered a detriment and a disadvantage by having to expend substantial sums to assess the extent, if any, of the physical damage to their website caused by appellants' intrusion. That the physical components were not damaged is fortunate, but it does not lessen the loss represented by consultant fees. Congress's use of the disjunctive, "damage or loss," confirms that it anticipated recovery in cases involving other than purely physical damage. But see In re Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1281 (C.D. Ca. 2001) (loss means "irreparable damage" and any other interpretation "would render the term 'damage' superfluous"); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 252 n.12

(S.D.N.Y. 2000) (lost business or goodwill could not constitute loss absent the impairment or unavailability of data or systems). To parse the words in any other way would not only impair Congress's intended scope of the Act, but would also serve to reward sophisticated intruders. As we move into an increasingly electronic world, the instances of physical damage will likely be fewer while the value to the victim of what has been stolen and the victim's costs in shoring up its security features undoubtedly will loom ever-larger. If we were to restrict the statute as appellants urge, we would flout Congress's intent by effectively permitting the CFAA to languish in the twentieth century, as violators of the Act move into the twenty-first century and beyond.

We do not hold, however, that any loss is compensable. The CFAA provides recovery for "damage" only if it results in a loss of at least $5,000. We agree with the court in _In re Doubleclick Inc. Privacy Litigation_, 154 F. Supp. 2d 497 (S.D.N.Y. 2001), that Congress could not have intended other types of loss to support recovery unless that threshold were met. Indeed, the Senate Report explicitly states that "if the loss to the victim meets the required monetary threshold," the victim is entitled to relief under the CFAA. S. Rep. 104-357, at 11. We therefore conclude that expenses of at least $5,000 resulting from a party's intrusion are "losses" for purposes of the "damage or loss" requirement of the CFAA.[18]

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.

[18] Only appellant Zefer raised the argument that the preliminary injunction violated the First Amendment. Explorica attempted to adopt that argument at oral argument. The lateness of Explorica's attempt renders it fruitless. See Garcia-Ayala v. Parenterals, Inc., 212 F.3d 638, 645 (1st Cir. 2000) (failure to brief an argument constitutes waiver despite attempt to raise the argument at oral argument); Piazza v. Aponte Roque, 909 F.2d 35, 37 (1st Cir. 1990) ("Except in extraordinary circumstances . . . a court of appeals will not consider an issue raised for the first time at oral argument.").