

386 F.3d 930

United States Court of Appeals,
Ninth Circuit.

CREATIVE COMPUTING, dba Internet
Truckstop.com, Plaintiff-Appellee,
v.
GETLOADED.COM LLC, and/or Codified
Corporation, Defendant-Appellant, and Jack C.
Martin, Defendant.

Filed Oct. 15, 2004.

Before: D.W. NELSON, KLEINFELD, and
FISHER, Circuit Judges.

KLEINFELD, Circuit Judge:

This case requires us to construe damages provisions in the Computer Fraud and Abuse Act.¹

Facts

Truck drivers and trucking companies try to avoid dead heading. “Deadheading” means having to drive a truck, ordinarily on a return trip, without a revenue-producing load. If the truck is moving, truck drivers and their companies want it to be carrying revenue-producing freight. In the past, truckers and shippers used blackboards to match up trips and loads. Eventually television screens were used instead of blackboards, but the matching was still inefficient. Better information on where the trucks and the loads are—and quick, easy access to that information—benefits shippers, carriers, and consumers.

Creative Computing developed a successful Internet site, truckstop.com, which it calls “The Internet Truckstop,” to match loads with trucks. The site is very easy to use. It has a feature called “radius search” that lets a truck driver in, say, Middletown, Connecticut, with some space in his truck, find within seconds all available loads in

whatever mileage radius he likes (and of course lets a shipper post a load so that a trucker with space can find it). The site was created so early in Internet history and worked so well that it came to dominate the load-board industry.

Getloaded decided to compete, but not honestly. After Getloaded set up a load-matching site, it wanted to get a bigger piece of Creative’s market. Creative wanted to prevent that, so it prohibited access to its site by competing loadmatching services. The Getloaded officers thought trucking companies would probably use the same login names and passwords on truckstop.com as they did on getloaded.com. Getloaded’s president, Patrick Hull, used the login name and password of a Getloaded subscriber, in effect impersonating the trucking company, to sneak into truckstop.com. Getloaded’s vice-president, Ken Hammond, accomplished the same thing by registering a defunct company, RFT Trucking, as a truckstop.com subscriber. These tricks enabled them to see all of the information available to Creative’s bona fide customers.

Getloaded’s officers also hacked into the code Creative used to operate its website. Microsoft had distributed a patch to prevent a hack it had discovered, but Creative Computing had not yet installed the patch on truckstop.com. Getloaded’s president and vice-president hacked into Creative Computing’s website through the back door that this patch would have locked. Once in, they examined the source code for the tremendously valuable radius-search feature.

Getloaded used a more old-fashioned trick to get unauthorized access to Creative Computing’s customer list. It hired away a Creative Computing employee who had given Getloaded an unauthorized tour of the truckstop.com website. This employee, while still working for Creative, accessed confidential information regarding several thousand of Creative’s customers. He downloaded, and sent to his home email account, the confidential address to truckstop.com’s server so that he could access the server from home and retrieve customer lists.

¹ 18 U.S.C. § 1030.

Creative Computing first discovered what Getloaded had done at a trade show in 1999. Getloaded was demonstrating a program that looked suspiciously like truckstop.com. Years later, it was clear why. During discovery, Creative uncovered a handwritten Getloaded employee's to-do list that included "mimic truckstop.com." After the Creative employee who had been feeding confidential information to Getloaded defected, Creative checked his computer and found evidence that he improperly accessed customer information before his departure.

Creative Computing sued Getloaded in district court for copyright infringement [and] Lanham Act violations. Creative also sought a temporary restraining order. The court granted a TRO that prohibited Getloaded from, among other things, removing or destroying evidence of how it had copied and used truckstop.com's source code, marketed to customers on Creative's customer list, or accessed the truckstop.com site. The parties stipulated to continuing the order in substantially the same form as a preliminary injunction while the litigation was pending. Subsequently, Creative amended its complaint, adding claims for damages under the federal Computer Fraud and Abuse Act.

The injunction did not work. Getloaded violated it. The district court made an express finding that "Getloaded acted in bad faith as its senior management—and others under its supervision and with its knowledge—lied under oath and violated the Court's injunction." The district judge carefully worked his way through contradictions in Patrick Hull's testimony, matching the testimony with truckstop.com's log of access to the site and the testimony of others who could have logged on at the critical times, thereby establishing that Hull had lied under oath. Expert testimony demonstrated to the judge that Getloaded had destroyed evidence that showed it had copied source code in violation of the injunction.

The case went to a jury trial. It turned out that none of truckstop.com's code was found in getloaded.com's code, so the jury's special verdict was for the defendant on the copyright claim.

Also, the site looked different enough that the special verdict was in favor of the defendant on the Lanham Act trade dress claim. But Creative Computing won anyway because the jury rendered special verdicts that Getloaded had violated the . . . Computer Fraud and Abuse Act. Damages awarded were . . . \$150,000 for each of three federal law violations The court also awarded \$300,000 in fees and \$42,787.35 in expenses as sanctions to compensate Creative Computing for the expense of figuring out and proving Getloaded's violations of the preliminary injunction and false statements in depositions. The court entered a permanent injunction extending indefinitely several provisions of the preliminary injunction, such as the prohibition against Getloaded's accessing truckstop.com. Getloaded appeals.

Analysis

I. The Computer Fraud and Abuse Act

Getloaded argues that no action could lie under the Computer Fraud and Abuse Act because it requires a \$5,000 floor for damages from each unauthorized access, and that Creative Computing submitted no evidence that would enable a jury to find that the floor was reached on any single unauthorized access. It relies for this argument on several district court cases that required \$5,000 damages from "a single act or event" and on a phrase in the Senate Report on the bill. Creative Computing cites several district court cases going the other way, but neither the parties nor we have found circuit court authority on point.

The briefs dispute which version of the statute we should apply—the one in effect when Getloaded committed the wrongs, or the one in effect when the case went to trial (which is still in effect). The old version of the statute made an exception to the fraudulent access provision if "the value of such use [unauthorized access to a protected computer] is not more than \$5,000 in

any 1-year period.”⁹ The new version, in effect now and during trial, says “loss ... during any 1-year period ... aggregating at least \$5,000 in value.”¹⁰ These provisions are materially identical.

The old version of the statute defined “damage” as “any impairment to the integrity or availability of data, a program, a system, or information” that caused the loss of at least \$5,000. It had no separate definition of “loss.” The new version defines “damage” the same way, but adds a definition of loss. “Loss” is defined in the new version as “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data ... and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service.”

For purposes of this case, we need not decide which version of the Act applies, because Getloaded loses either way. Neither version of the statute supports a construction that would require proof of \$5,000 of damage or loss from a single unauthorized access. The syntax makes it clear that in both versions, the \$5,000 floor applies to how much damage or loss there is to the victim over a one-year period, not from a particular intrusion. Getloaded argues that “impairment” is singular, so the floor has to be met by a single intrusion. The premise does not lead to the conclusion. The statute (both the earlier and the current versions) says “damage”

means “any impairment to the integrity or availability of data[etc.] ... that causes loss aggregating at least \$5,000.” Multiple intrusions can cause a single impairment, and multiple corruptions of data can be described as a single “impairment” to the data. The statute does not say that an “impairment” has to result from a single intrusion, or has to be a single corrupted byte. A court construing a statute attributes a rational purpose to Congress. Getloaded’s construction would attribute obvious futility to Congress rather than rationality, because a hacker could evade the statute by setting up thousands of \$4,999 (or millions of \$4.99) intrusions. As the First Circuit pointed out in the analogous circumstance of physical impairment, so narrow a construction of the \$5,000 impairment requirement would merely “reward sophisticated intruders.” The damage floor in the Computer Fraud and Abuse Act contains no “single act” requirement.

Getloaded’s scrap of legislative history is a remark in the Senate Report that “the Committee intends to make clear that losses caused by the same act may be aggregated for purposes of meeting the ... threshold.” The obvious purpose of this remark was permissive, to allow aggregation to meet the \$5,000 floor, as when one intrusion causes one expense after another for months. Getloaded wants us to read the remark restrictively instead of permissively, to mean that the \$5,000 floor has to be reached from a single intrusion. This seems a fine example of an unambiguous statute to which we are asked to apply an ambiguous snippet of legislative history. “It makes no sense to parse the ambiguous legislative history as though it were the law. The preferable way to resolve linguistic ambiguity is to evaluate the alternative readings in light of the purpose of the statute.”

[. . .]

AFFIRMED.

⁹ 18 U.S.C. § 1030(a)(4) (2001) (“[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.”).

¹⁰ 18 U.S.C. § 1030(a)(5)(B)(i) (“[Whoever caused] loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$5,000 in value.”).