

440 F.3d 418

United States Court of Appeals,
Seventh Circuit.

INTERNATIONAL AIRPORT CENTERS,

L.L.C., et al., Plaintiffs-Appellants,

v.

Jacob **CITRIN,** Defendant-Appellee.

Decided March 8, 2006.

Before POSNER, WILLIAMS, and SYKES,
Circuit Judges.

POSNER, Circuit Judge.

This appeal from the dismissal of the plaintiffs' suit for failure to state a claim mainly requires us to interpret the word "transmission" in a key provision of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. The complaint alleges the following facts, which for purposes of deciding the appeal we must take as true. The defendant, Citrin, was employed by the plaintiffs—affiliated companies engaged in the real estate business that we'll treat as one to simplify the opinion, and call "IAC"—to identify properties that IAC might want to acquire, and to assist in any ensuing acquisition. IAC lent Citrin a laptop to use to record data that he collected in the course of his work in identifying potential acquisition targets.

Citrin decided to quit IAC and go into business for himself, in breach of his employment contract. Before returning the laptop to IAC, he deleted all the data in it—not only the data that he had collected but also data that would have revealed to IAC improper conduct in which he had engaged before he decided to quit. Ordinarily, pressing the "delete" key on a computer (or using a mouse click to delete) does not affect the data sought to be deleted; it merely removes the index entry and pointers to the data file so that the file appears no longer to be there, and the space allocated to that file is made available for future write commands. Such "deleted" files are easily recoverable. But Citrin

loaded into the laptop a secure-erasure program, designed, by writing over the deleted files, to prevent their recovery. Thomas J. Fitzgerald, "Deleted But Not Gone: Programs Help Protect Confidential Data by Making Disks and Drives Unreadable," *New York Times* (national ed.), Nov. 3, 2005, p. C9. IAC had no copies of the files that Citrin erased.

The provision of the Computer Fraud and Abuse Act on which IAC relies provides that whoever "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer [a defined term that includes the laptop that Citrin used]," violates the Act. 18 U.S.C. § 1030(a)(5)(A)(i). Citrin argues that merely erasing a file from a computer is not a "transmission." Pressing a delete or erase key in fact transmits a command, but it might be stretching the statute too far (especially since it provides criminal as well as civil sanctions for its violation) to consider any typing on a computer keyboard to be a form of "transmission" just because it transmits a command to the computer.

There is more here, however: the transmission of the secure-erasure program to the computer. We do not know whether the program was downloaded from the Internet or copied from a floppy disk (or the equivalent of a floppy disk, such as a CD) inserted into a disk drive that was either inside the computer or attached to it by a wire. Oddly, the complaint doesn't say; maybe IAC doesn't know—maybe all it knows is that when it got the computer back, the files in it had been erased. But we don't see what difference the precise mode of transmission can make. In either the Internet download or the disk insertion, a program intended to cause damage (not to the physical computer, of course, but to its files—but "damage" includes "any impairment to the integrity or availability of data, a program, a system, or information," 18 U.S.C. § 1030(e)(8)) is transmitted to the computer electronically. The only difference, so far as the mechanics of transmission are concerned, is that the disk is inserted manually before the program on it is transmitted electronically to the computer. The

difference vanishes if the disk drive into which the disk is inserted is an external drive, connected to the computer by a wire, just as the computer is connected to the Internet by a telephone cable or a broadband cable or wirelessly.

There is the following contextual difference between the two modes of transmission, however: transmission via disk requires that the malefactor have physical access to the computer. By using the Internet, Citrin might have erased the laptop's files from afar by transmitting a virus. Such long-distance attacks can be more difficult to detect and thus to deter or punish than ones that can have been made only by someone with physical access, usually an employee. The inside attack, however, while easier to detect may also be easier to accomplish. Congress was concerned with both types of attack: attacks by virus and worm writers, on the one hand, which come mainly from the outside, and attacks by disgruntled programmers who decide to trash the employer's data system on the way out (or threaten to do so in order to extort payments), on the other. If the statute is to reach the disgruntled programmer, which Congress intended by providing that whoever "intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage" violates the Act, 18 U.S.C. § 1030(a)(5)(A)(ii) (emphasis added), it can't make any difference that the destructive program comes on a physical medium, such as a floppy disk or CD.

Citrin violated that subsection too. For his authorization to access the laptop terminated when, having already engaged in misconduct and decided to quit IAC in violation of his employment contract, he resolved to destroy files that incriminated himself and other files that were also the property of his employer, in violation of the duty of loyalty that agency law imposes on an employee. *United States v. Galindo*, 871 F.2d 99, 101 (9th Cir.1989); *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F.Supp.2d 1121, 1124-25 (W.D. Wash.2000); see Restatement (Second) of Agency §§ 112, 387 (1958).

Muddying the picture some, the Computer Fraud and Abuse Act distinguishes between "without authorization" and "exceeding authorized access," 18 U.S.C. §§ 1030(a)(1), (2), (4), and, while making both punishable, defines the latter as "access[ing] a computer with authorization and ... us[ing] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." § 1030(e)(6). That might seem the more apt description of what Citrin did.

The difference between "without authorization" and "exceeding authorized access" is paper thin, see *Pacific Aerospace & Electronics, Inc. v. Taylor*, 295 F.Supp.2d 1188, 1196-97 (E.D.Wash.2003), but not quite invisible. In *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 583-84 (1st Cir.2001), for example, the former employee of a travel agent, in violation of his confidentiality agreement with his former employer, used confidential information that he had obtained as an employee to create a program that enabled his new travel company to obtain information from his former employer's website that he could not have obtained as efficiently without the use of that confidential information. The website was open to the public, so he was authorized to use it, but he exceeded his authorization by using confidential information to obtain better access than other members of the public.

Our case is different. Citrin's breach of his duty of loyalty terminated his agency relationship (more precisely, terminated any rights he might have claimed as IAC's agent—he could not by unilaterally terminating any duties he owed his principal gain an advantage!) and with it his authority to access the laptop, because the only basis of his authority had been that relationship. "Violating the duty of loyalty, or failing to disclose adverse interests, voids the agency relationship." *State v. DiGiulio*, 835 P.2d 488, 492 (App.1992). "Unless otherwise agreed, the authority of the agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal." *Id.*; Restatement, *supra*, § 112; see also *Shurgard*

Storage Centers, Inc. v. Safeguard Self Storage, Inc., supra, 119 F.Supp.2d at 1123, 1125; cf. *Phansalkar v. Andersen Weinroth & Co.*, 344 F.3d 184, 201-02 (2d Cir.2003) (per curiam); Restatement, supra, § 409(1) and comment b and illustration 2.

Citrin points out that his employment contract authorized him to “return or destroy “ data in the laptop when he ceased being employed by IAC (emphasis added). But it is unlikely, to say the least, that the provision was intended to authorize him to destroy data that he knew the company had no duplicates of and would have wanted to have—if only to nail Citrin for misconduct. The purpose of the provision may have been to avoid overloading the company with returned data of no further value, which the employee should simply have deleted. More likely the purpose was simply to remind Citrin that he was not to disseminate confidential data after he left the company’s employ—the provision authorizing him to return or destroy data in the laptop was limited to “Confidential” information. There may be a dispute over whether the incriminating files that Citrin destroyed contained “confidential” data, but that issue cannot be resolved on this appeal.

The judgment is reversed with directions to reinstate the suit, including the supplemental claims that the judge dismissed because he was dismissing IAC’s federal claim.

REVERSED AND REMANDED.