United States v. Morris

928 F.2d 504 (2nd. Cir. 1991)

Before NEWMAN and WINTER, Circuit Judges, and DALY, District Judge.[1]

This appeal presents two narrow issues of statutory construction concerning a provision Congress recently adopted to strengthen protection against computer crimes. Section 2(d) of the Computer Fraud and Abuse Act of 1986, 18 U.S.C. Section 1030(a)(5)(A) (1988), punishes anyone who intentionally accesses without authorization a category of computers known as "[f]ederal interest computers" and damages or prevents authorized use of information in such computers, causing loss of $1,000 or more. The issues raised are (1) whether the Government must prove not only that the defendant intended to access a federal interest computer, but also that the defendant intended to prevent authorized use of the computer's information and thereby cause loss; and (2) what satisfies the statutory requirement of "access without authorization."

These questions are raised on an appeal by Robert Tappan Morris from the May 16, 1990, judgment of the District Court for the Northern District of New York (Howard G. Munson, Judge) convicting him, after a jury trial, of violating 18 U.S.C. Section 1030(a)(5)(A). Morris released into Internet, a national computer network, a computer program known as a "worm"[2] that spread and multiplied, eventually causing computers at various educational institutions and military sites to "crash" or cease functioning.

We conclude that section 1030(a)(5)(A) does not require the Government to demonstrate that the defendant intentionally prevented authorized use and thereby caused loss. We also find that there was sufficient evidence for the jury to conclude that Morris acted "without authorization" within the meaning of section 1030(a)(5)(A). We therefore affirm.

FACTS

In the fall of 1988, Morris was a first-year graduate student in Cornell University's computer science Ph.D. program. Through undergraduate work at Harvard and in various jobs he had acquired significant computer experience and expertise. When Morris entered Cornell, he was given an account on the computer at the Computer Science Division. This account gave him explicit authorization to use computers at Cornell. Morris engaged in various discussions with fellow graduate students about the security of computer networks and his ability to penetrate it.

In October 1988, Morris began work on a computer program, later known as the Internet "worm" or "virus." The goal of this program was to demonstrate the inadequacies of current security measures on computer networks by exploiting the security defects that Morris had discovered. The tactic he selected was release of a worm into network computers. Morris designed the program to spread across a national network of computers after being inserted at one computer location connected to the network. Morris released the worm into Internet, which is a group of national networks that connect university, governmental, and military computers around the country. The network permits communication and transfer of information between computers on the network.

---

[1] The Honorable T.F. Gilroy Daly of the District Court for the District of Connecticut, sitting by designation.

[2] In the colorful argot of computers, a "worm" is a program that travels from one computer to another but does not attach itself to the operating system of the computer it "infects." It differs from a "virus," which is also a migrating program, but one that attaches itself to the operating system of any computer it enters and can infect any other computer that uses files from the infected computer.

Morris sought to program the Internet worm to spread widely without drawing attention to itself. The worm was supposed to occupy little computer operation time, and thus not interfere with normal use of the computers. Morris programmed the worm to make it difficult to detect and read, so that other programmers would not be able to "kill" the worm easily. Morris also wanted to ensure that the worm did not copy itself onto a computer that already had a copy. Multiple copies of the worm on a computer would make the worm easier to detect and would bog down the system and ultimately cause the computer to crash. Therefore, Morris designed the worm to "ask" each computer whether it already had a copy of the worm. If it responded "no," then the worm would copy onto the computer; if it responded "yes," the worm would not duplicate. However, Morris was concerned that other programmers could kill the worm by programming their own computers to falsely respond "yes" to the question. To circumvent this protection, Morris programmed the worm to duplicate itself every seventh time it received a "yes" response. As it turned out, Morris underestimated the number of times a computer would be asked the question, and his one-out-of-seven ratio resulted in far more copying than he had anticipated. The worm was also designed so that it would be killed when a computer was shut down, an event that typically occurs once every week or two. This would have prevented the worm from accumulating on one computer, had Morris correctly estimated the likely rate of reinfection.

Morris identified four ways in which the worm could break into computers on the network: (1) through a "hole" or "bug" (an error) in SEND MAIL, a computer program that transfers and receives electronic mail on a computer; (2) through a bug in the "finger demon" program, a program that permits a person to obtain limited information about the users of another computer; (3) through the "trusted hosts" feature, which permits a user with certain privileges on one computer to have equivalent privileges on another computer without using a password; and (4) through a program of password guessing, whereby various combinations of letters are tried out in rapid sequence in the hope that one will be an authorized user's password, which is entered to permit whatever level of activity that user is authorized to perform.

On November 2, 1988, Morris released the worm from a computer at the Massachusetts Institute of Technology. MIT was selected to disguise the fact that the worm came from Morris at Cornell. Morris soon discovered that the worm was replicating and reinfecting machines at a much faster rate than he had anticipated. Ultimately, many machines at locations around the country either crashed or became "catatonic." When Morris realized what was happening, he contacted a friend at Harvard to discuss a solution. Eventually, they sent an anonymous message from Harvard over the network, instructing programmers how to kill the worm and prevent reinfection. However, because the network route was clogged, this message did not get through until it was too late. Computers were affected at numerous installations, including leading universities, military sites, and medical research facilities. The estimated cost of dealing with the worm at each installation ranged from $200 to more than $53,000.

Morris was found guilty, following a jury trial, of violating 18 U.S.C. Section 1030(a)(5)(A). He was sentenced to three years of probation, 400 hours of community service, a fine of $10,050, and the costs of his supervision.

DISCUSSION

I. The intent requirement in section 1030(a)(5)(A)

Section 1030(a)(5)(A), covers anyone who (5) intentionally accesses a Federal interest computer without authorization, and by means of one or more instances of such conduct alters, damages, or destroys information in any such Federal interest computer, or prevents authorized use of any such computer or information, and thereby (A) causes loss to one or more others of a value aggregating $1,000 or more during any one year period; ... [emphasis added].

The District Court concluded that the intent requirement applied only to the accessing and not to the resulting damage. Judge Munson found recourse to legislative history unnecessary because he considered the statute clear and unambiguous. However, the Court observed that the legislative history supported its reading of section 1030(a)(5)(A).

Morris argues that the Government had to prove not only that he intended the unauthorized access of a federal interest computer, but also that he intended to prevent others from using it, and thus cause a loss. The adverb "intentionally," he contends, modifies both verb phrases of the section. The Government urges that since punctuation sets the "accesses" phrase off from the subsequent "damages" phrase, the provision unambiguously shows that "intentionally" modifies only "accesses." Absent textual ambiguity, the Government asserts that recourse to legislative history is not appropriate. See Burlington N.R. Co. v. Oklahoma Tax Comm'n, 481 U.S. 454, 461, 107 S.Ct. 1855, 1859, 95 L.Ed.2d 404 (1987); Consumer Product Safety Comm'n v. GTE Sylvania, Inc., 447 U.S. 102, 108, 100 S.Ct. 2051, 2056, 64 L.Ed.2d 766 (1980); United States v. Holroyd, 732 F.2d 1122, 1125 (2d Cir. 1984).

With some statutes, punctuation has been relied upon to indicate that a phrase set off by commas is independent of the language that followed. See United States v. Ron Pair Enterprises, Inc., 489 U.S. 235, 241, 109 S.Ct. 1026, 1030, 103 L.Ed.2d 290 (1989) (interpreting the Bankruptcy Code). However, we have been advised that punctuation is not necessarily decisive in construing statutes, see Costanzo v. Tillinghast, 287 U.S. 341, 344, 53 S.Ct. 152, 153, 77 L.Ed. 350 (1932), and with many statutes, a mental state adverb adjacent to initial words has been applied to phrases or clauses appearing later in the statute without regard to the punctuation or structure of the statute. See Liparota v. United States, 471 U.S. 419, 426-29, 105 S.Ct. 2084, 2088-90, 85 L.Ed.2d 434 (1985) (interpreting food stamps provision); United States v. Nofziger, 878 F.2d 442, 446-50 (D.C.Cir.) (interpreting government "revolving door" statute), cert. denied, --- U.S. ----, 110 S.Ct. 564, 107 L.Ed.2d 559 (1989); United States v. Johnson & Towers, Inc., 741 F.2d 662, 667-69 (3d Cir. 1984) (interpreting the conservation act), cert. denied, 469 U.S. 1208, 105 S.Ct. 1171, 84 L.Ed.2d 321 (1985). In the present case, we do not believe the comma after "authorization" renders the text so clear as to preclude review of the legislative history.

The first federal statute dealing with computer crimes was passed in 1984, Pub.L. No. 98-473 (codified at 18 U.S.C. Section 1030 (Supp. II 1984)). The specific provision under which Morris was convicted was added in 1986, Pub.L. No. 99-474, along with some other changes. The 1986 amendments made several changes relevant to our analysis.

First, the 1986 amendments changed the scienter requirement in section 1030(a)(2) from "knowingly" to "intentionally." SeePub.L. No. 99-474, section 2(a)(1). The subsection now covers anyone who (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.). According to the Senate Judiciary Committee, Congress changed the mental state requirement in section 1030(a)(2) for two reasons. Congress sought only to proscribe intentional acts of unauthorized access,

not "mistaken, inadvertent, or careless" acts of unauthorized access. S.Rep. No. 99-432, 99th Cong., 2d Sess. 5 (1986), reprinted in 1986 U.S. Code Cong. & Admin. News 2479, 2483 [hereinafter Senate Report].

Also, Congress expressed concern that the "knowingly" standard "might be inappropriate for cases involving computer technology." Id. The concern was that a scienter requirement of "knowingly" might encompass the acts of an individual "who inadvertently 'stumble[d] into' someone else's computer file or computer data," especially where such individual was authorized to use a particular computer. Id. at 6, 1986 U.S.Code Cong. & Admin.News at 2483. The Senate Report concluded that "[t]he substitution of an 'intentional' standard is designed to focus Federal criminal prosecutions on those whose conduct evinces a clear intent to enter, without proper authorization, computer files or data belonging to another." Id., U.S.Code Cong. & Admin.News at 2484. Congress retained the "knowingly" standard in other subsections of section 1030. See 18 U.S.C. Section 1030(a)(1), (a)(4).

This use of a mens rea standard to make sure that inadvertent accessing was not covered is also emphasized in the Senate Report's discussion of section 1030(a)(3) and section 1030(a)(5), under which Morris was convicted. Both subsections were designed to target "outsiders," individuals without authorization to access any federal interest computer. Senate Report at 10, U.S.Code Cong. & Admin.News at 2488. The rationale for the mens rea requirement suggests that it modifies only the "accesses" phrase, which was the focus of Congress's concern in strengthening the scienter requirement.

The other relevant change in the 1986 amendments was the introduction of subsection (a)(5) to replace its earlier version, subsection (a)(3) of the 1984 act, 18 U.S.C. Section 1030(a)(3) (Supp. II 1984). The predecessor subsection covered anyone who knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and by means of such conduct knowingly uses, modifies, destroys, or discloses information in, or prevents authorized use of, such computer, if such computer is operated for or on behalf of the Government of United States and such conduct affects such operation. The 1986 version changed the mental state requirement from "knowingly" to "intentionally," and did not repeat it after the "accesses" phrase, as had the 1984 version. By contrast, other subsections of section 1030 have retained "dual intent" language, placing the scienter requirement at the beginning of both the "accesses" phrase and the "damages" phrase. See, e.g., 18 U.S.C. Section 1030(a)(1).

Morris notes the careful attention that Congress gave to selecting the scienter requirement for current subsections (a)(2) and (a)(5). Then, relying primarily on comments in the Senate and House reports, Morris argues that the "intentionally" requirement of section 1030(a)(5)(A) describes both the conduct of accessing and damaging. As he notes, the Senate Report said that "[t]he new subsection 1030(a)(5) to be created by the bill is designed to penalize those who intentionally alter, damage, or destroy certain computerized data belonging to another." Senate Report at 10, U.S.Code Cong. & Admin.News at 2488. The House Judiciary Committee stated that "the bill proposes a new section (18 U.S.C. 1030(a)(5)) which can be characterized as a 'malicious damage' felony violation involving a Federal interest computer. We have included an 'intentional' standard for this felony and coverage is extended only to outside trespassers with a $1,000 threshold damage level." H.R.Rep. No. 99-612, 99th Cong.2d Sess. at 7 (1986). A member of the Judiciary Committee also referred to the section 1030(a)(5) offense as a "malicious damage" felony during the floor debate. 132 Cong.Rec. H3275, 3276 (daily ed. June 3, 1986) (remarks of Rep. Hughes).

The Government's argument that the scienter requirement in section 1030(a)(5)(A) applies only to the "accesses" phrase is premised primarily upon the difference between subsection (a)(5)(A) and its predecessor in the 1984 statute. The decision to state the scienter requirement only once in subsection (a)(5)(A), along with the decision to change it from "knowingly" to "intentionally," are claimed to evince a clear intent upon the part of Congress to apply the scienter requirement only to the "accesses" phrase, though making that requirement more difficult to satisfy. This reading would carry out the Congressional objective of protecting the individual who "inadvertently 'stumble[s] into' someone else's computer file." Senate Report at 6, U.S. Code Cong. & Admin. News at 2483.

The Government also suggests that the fact that other subsections of section 1030 continue to repeat the scienter requirement before both phrases of a subsection is evidence that Congress selectively decided within the various subsections of section 1030 where the scienter requirement was and was not intended to apply. Morris responds with a plausible explanation as to why certain other provisions of section 1030 retain dual intent language. Those subsections use two different mens rea standards; therefore it is necessary to refer to the scienter requirement twice in the subsection. For example, section 1030(a)(1) covers anyone who (1) knowingly accesses a computer without authorization or exceeds authorized access, and by means of such conduct obtains information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data ... with the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation.

Since Congress sought in subsection (a)(1) to have the "knowingly" standard govern the "accesses" phrase and the "with intent" standard govern the "results" phrase, it was necessary to state the scienter requirement at the beginning of both phrases. By contrast, Morris argues, where Congress stated the scienter requirement only once, at the beginning of the "accesses" phrase, it was intended to cover both the "accesses" phrase and the phrase that followed it.

There is a problem, however, with applying Morris's explanation to section 1030(a)(5)(A). As noted earlier, the predecessor of subsection (a)(5)(A) explicitly placed the same mental state requirement before both the "accesses" phrase and the "damages" phrase. In relevant part, that predecessor in the 1984 statute covered anyone who "knowingly accesses a computer without authorization, ... and by means of such conduct knowingly uses, modifies, destroys, or discloses information in, or prevents authorized use of, such computer...." 18 U.S.C. Section 1030(a)(3) (Supp. II 1984) (emphasis added). This earlier provision demonstrates that Congress has on occasion chosen to repeat the same scienter standard in the "accesses" phrase and the subsequent phrase of a subsection of the Computer Fraud Statute. More pertinently, it shows that the 1986 amendments adding subsection (a)(5)(A) placed the scienter requirement adjacent only to the "accesses" phrase in contrast to a predecessor provision that had placed the same standard before both that phrase and the subsequent phrase.

Despite some isolated language in the legislative history that arguably suggests a scienter component for the "damages" phrase of section 1030(a)(5)(A), the wording, structure, and purpose of the subsection, examined in comparison with its departure from the format of its predecessor provision persuade us that the "intentionally" standard applies only to the "accesses" phrase of section 1030(a)(5)(A), and not to its "damages" phrase.

II. The unauthorized access requirement in section 1030(a)(5)(A)

Section 1030(a)(5)(A) penalizes the conduct of an individual who "intentionally accesses a Federal interest computer without authorization." Morris contends that his conduct constituted, at most, "exceeding authorized access" rather than the "unauthorized access" that the subsection punishes. Morris argues that there was insufficient evidence to convict him of "unauthorized access," and that even if the evidence sufficed, he was entitled to have the jury instructed on his "theory of defense."

We assess the sufficiency of the evidence under the traditional standard. Morris was authorized to use computers at Cornell, Harvard, and Berkeley, all of which were on INTERNET. As a result, Morris was authorized to communicate with other computers on the network to send electronic mail (SEND MAIL), and to find out certain information about the users of other computers (finger demon). The question is whether Morris's transmission of his worm constituted exceeding authorized access or accessing without authorization.

The Senate Report stated that section 1030(a)(5)(A), like the new section 1030(a)(3), would "be aimed at 'outsiders,' i.e., those lacking authorization to access any Federal interest computer." Senate Report at 10, U.S.Code Cong. & Admin.News at 2488. But the Report also stated, in concluding its discussion on the scope of section 1030(a)(3), that it applies "where the offender is completely outside the Government, ... or where the offender's act of trespass is interdepartmental in nature." Id. at 8, U.S.Code Cong. & Admin.News at 2486 (emphasis added).

Morris relies on the first quoted portion to argue that his actions can be characterized only as exceeding authorized access, since he had authorized access to a federal interest computer. However, the second quoted portion reveals that Congress was not drawing a bright line between those who have some access to any federal interest computer and those who have none. Congress contemplated that individuals with access to some federal interest computers would be subject to liability under the computer fraud provisions for gaining unauthorized access to other federal interest computers. See, e.g., id. (stating that a Labor Department employee who uses Labor's computers to access without authorization an FBI computer can be criminally prosecuted).

The evidence permitted the jury to conclude that Morris's use of the SEND MAIL and finger demon features constituted access without authorization. While a case might arise where the use of SEND MAIL or finger demon falls within a nebulous area in which the line between accessing without authorization and exceeding authorized access may not be clear, Morris's conduct here falls well within the area of unauthorized access. Morris did not use either of those features in any way related to their intended function. He did not send or read mail nor discover information about other users; instead he found holes in both programs that permitted him a special and unauthorized access route into other computers.

Moreover, the jury verdict need not be upheld solely on Morris's use of SEND MAIL and finger demon. As the District Court noted, in denying Morris' motion for acquittal, Although the evidence may have shown that defendant's initial insertion of the worm simply exceeded his authorized access, the evidence also demonstrated that the worm was designed to spread to other computers at which he had no account and no authority, express or implied, to unleash the worm program. Moreover, there was also evidence that the worm was designed to gain access to computers at which he had no account by guessing their passwords. Accordingly, the evidence did support the jury's conclusion that defendant accessed without authority as opposed to merely exceeding the scope of his authority. In light of the reasonable conclusions that the jury could draw from Morris's use of SEND MAIL and finger demon, and

from his use of the trusted hosts feature and password guessing, his challenge to the sufficiency of the evidence fails.

Morris endeavors to bolster his sufficiency argument by contending that his conduct was not punishable under subsection (a)(5) but was punishable under subsection (a)(3). That concession belies the validity of his claim that he only exceeded authorization rather than made unauthorized access. Neither subsection (a)(3) nor (a)(5) punishes conduct that exceeds authorization. Both punish a person who "accesses" "without authorization" certain computers. Subsection (a)(3) covers the computers of a department or agency of the United States; subsection (a)(5) more broadly covers any federal interest computers, defined to include, among other computers, those used exclusively by the United States, 18 U.S.C. Section 1030(e)(2)(A), and adds the element of causing damage or loss of use of a value of $1,000 or more. If Morris violated subsection (a)(3), as he concedes, then his conduct in inserting the worm into the Internet must have constituted "unauthorized access" under subsection (a)(5) to the computers of the federal departments the worm reached, for example, those of NASA and military bases.

To extricate himself from the consequence of conceding that he made "unauthorized access" within the meaning of subsection (a)(3), Morris subtly shifts his argument and contends that he is not within the reach of subsection (a)(5) at all. He argues that subsection (a)(5) covers only those who, unlike himself, lack access to any federal interest computer. It is true that a primary concern of Congress in drafting subsection (a)(5) was to reach those unauthorized to access any federal interest computer. The Senate Report stated, "[T]his subsection [(a)(5)] will be aimed at 'outsiders,' i.e., those lacking authorization to access any Federal interest computer." Senate Report at 10, U.S. Code Cong. & Admin. News at 2488. But the fact that the subsection is "aimed" at such "outsiders" does not mean that its coverage is limited to them. Congress understandably thought that the group most likely to damage federal interest computers would be those who lack authorization to use any of them. But it surely did not mean to insulate from liability the person authorized to use computers at the State Department who causes damage to computers at the Defense Department. Congress created the misdemeanor offense of subsection (a)(3) to punish intentional trespasses into computers for which one lacks authorized access; it added the felony offense of subsection (a)(5) to punish such a trespasser who also causes damage or loss in excess of $1,000, not only to computers of the United States but to any computer within the definition of federal interest computers. With both provisions, Congress was punishing those, like Morris, who, with access to some computers that enable them to communicate on a network linking other computers, gain access to other computers to which they lack authorization and either trespass, in violation of subsection (a)(3), or cause damage or loss of $1,000 or more, in violation of subsection (a)(5).

Morris also contends that the District Court should have instructed the jury on his theory that he was only exceeding authorized access. The District Court decided that it was unnecessary to provide the jury with a definition of "authorization." We agree. Since the word is of common usage, without any technical or ambiguous meaning, the Court was not obliged to instruct the jury on its meaning. See, e.g., United States v. Chenault, 844 F.2d 1124, 1131 (5th Cir. 1988) ("A trial court need not define specific statutory terms unless they are outside the common understanding of a juror or are so technical or specific as to require a definition.").

An instruction on "exceeding authorized access" would have risked misleading the jury into thinking that Morris could not be convicted if some of his conduct could be viewed as falling within this description. Yet, even if that phrase might have applied to some of his conduct, he could nonetheless be found liable for doing what the statute prohibited, gaining access where he was unauthorized and causing loss.

Additionally, the District Court properly refused to charge the jury with Morris's proposed jury instruction on access without authorization. That instruction stated, "To establish the element of lack of authorization, the government must prove beyond a reasonable doubt that Mr. Morris was an 'outsider,' that is, that he was not authorized to access any Federal interest computer in any manner." As the analysis of the legislative history reveals, Congress did not intend an individual's authorized access to one federal interest computer to protect him from prosecution, no matter what other federal interest computers he accesses.

CONCLUSION