United States v. Morris

United States Court of Appeals for the Second Circuit

December 4, 1990, Argued ; March 7, 1991, Decided

No. 90-1336

Reporter
928 F.2d 504 *; 1991 U.S. App. LEXIS 3682 **

UNITED STATES OF AMERICA, Appellee, v. ROBERT TAPPAN MORRIS, Defendant-Appellant

Opinion

[*505] […]

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. § 1030(a)(5)(A) **[**2]** (1988)* […]. The issues raised are […] (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. § 1030(a)(5)(A)*. Morris released into INTERNET, a national computer network, a computer program known as a "worm" [11] that spread and multiplied, eventually causing computers at various educational institutions and military sites to "crash" or cease functioning.

[3]** We […] 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. […] 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 **[**4]** 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.

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.

[*506] 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 **[**5]** "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. […]

---

[11] 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 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; **[**6]**
>
> (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 **[**7]** 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. § 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

[…]

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 was authorized to **[**18]** 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 **[*510]** (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, **[**19]** 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 **[**20]** 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.

[…]

CONCLUSION

For the foregoing reasons, the judgment of the District Court is affirmed.