12-22-2006

USA v. Carlson

Precedential or Non-Precedential: Non-Precedential

Docket No. 05-3562

NOT PRECEDENTIAL

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

No. 05-3562

UNITED STATES OF AMERICA,

Appellee,

v.

ALLAN CARLSON,

Appellant.

On Appeal from the Judgment of the United States District Court
for the Eastern District of Pennsylvania
(D.C. No. Crim. 05-3562)
District Judge: Honorable Berle M. Schiller

Submitted Under Third Circuit LAR 34.1(a)
December 12, 2006

Before: SMITH, ROTH, *Circuit Judges*, and IRENAS,[*] *Senior District Judge.*

(Filed December 22, 2006)

---

[*] Honorable Joseph E. Irenas, Senior United States District Judge for the District of New Jersey, sitting by designation.

OPINION

IRENAS, *Senior United States District Judge.*

On July 14, 2005, the District Court for the Eastern District of Pennsylvania imposed upon Appellant Allan Eric Carlson a sentence of 48 months imprisonment, a term of supervised release of three years, restitution of $14,970.63, and a special assessment of $7,900.00 after a jury found him guilty of computer and identification fraud in violation of 18 U.S.C. § 1030(a)(5)(A)(I) & (ii) (the "Computer Fraud and Abuse Act") and 18 U.S.C. § 1028(a)(7)(the "Identity and Information Fraud Act").[1] Carlson appeals the order denying his Fed. R. Crim. P. 29 motion for judgment of acquittal. The basis for his motion was insufficiency of the evidence brought against him under the Computer Fraud and Information Act.[2] We will affirm.

I.

This Court has jurisdiction to review the order of judgment in a criminal case pursuant to 28 U.S.C. § 1291. We exercise *de novo* review of the District Court's denial of Carlson's motion for judgment of acquittal. *Unites States v. Flores*, 454 F.3d 149, 154

[1] Specifically, the jury convicted Carlson of 26 counts of intentionally causing damage to a protected computer, 26 counts of knowingly making unauthorized access to a protected computer and thereby recklessly causing damage, and 27 counts of identity fraud.

[2] Carlson does not contest his conviction stemming from his violation of the Identification and Information Fraud Act, 18 U.S.C. § 1028(a)(7).

(3d Cir. 2006).

II.

Prior to his arrest and conviction, Carlson was an avid Philadelphia Phillies fan living in California. (Appellant's Brief, 2). He became savvy with internet use and technology in 1999, and in 2000 began posting messages on online bulletin boards devoted to the Philadelphia Phillies as a way to communicate with other Phillies fans. (JA 3.139- 44).

Beginning in 2001, Carlson engaged in two types of e-mail activities that caused damage to other internet users: "direct attack" e-mailing, in which Carlson sent thousands of e-mails to one particular e-mail address,[3] and "indirect attack" e-mailing, where he sent one e-mail to many e-mail addresses.[4]

In employing the direct attack method, Carlson sent thousands of e-mails mainly to a few e-mail addresses at the Philadelphia Phillies. Although the 'from' field indicated that the e-mails were sent from various e-mail addresses not his own,[5] such as the FBI and

---

[3] The Government referred to such tactics as "direct attacks" on individual e-mail users, as the user's e-mail inbox would immediately flood with e-mails sent by Carlson through a third party's IP address.

[4] The Government referred to this as an "indirect attack," in that it did not flood any one e-mail user's account immediately, but rather would flood the sender's e-mail address when e-mails sent to invalid addresses were bounced back to the sender. Because Carlson sent e-mails from addresses of other internet users, e-mails would be bounced back to those inboxes, rather than the inbox of Carlson.

[5] This act is referred to as "spoofing."

the Philadelphia Phillies, they were not sent from those individuals and entities, but rather by Carlson using the Internet Protocol ("IP") addresses of other computers. Carlson claims that he sent these e-mails in an attempt to inform journalists and Phillies management about issues with the management of the Phillies that he considered problematic, and to start conversations among other internet users concerning such problems. The evidence produced at trial showed that while some e-mails concerned the Phillies, others did not.

Examples of Carlson's direct attacks are as follows. On November 7, 2001, Carlson sent 1,168 e-mails entitled "The Mariner's Didn't Trade A-Rod" from "SpecialProsecutor@fbi.gov," an e-mail address belonging to a Canadian internet user, to six writers at Philadelphia Newspapers, Inc. ("PNI"). (JA 1.112, Supp. App. 4). On November 11, 2001, Carlson sent over 5,000 e-mails entitled "Sign JASON GIAMBI" to one address at the Phillies. (JA 2.107-113; Supp. App. 44-45). On March 12, Carlson sent 1,800 e-mails to one address at the Phillies, and another 1,800 e-mails to another Phillies' address. (JA 2.115-7, 2.128-9; Supp. App. 44). On March 14, 2002, Carlson sent an e-mail entitled "The Color of Crime" about raced-based crimes to 5,514 employees of PNI. The e-mails appeared to be from either Lillian Swanson, Ombudsman of the Philadelphia Inquirer, or Walker Lundy, an editor of the Inquirer. (JA 1.143-45; Supp. App. 43, 49, 66-134).

When employing the indirect attack method, Carlson would send spam e-mails

from spoofed accounts to thousands of people whose addresses he collected primarily by using computer software.[6] For example, On November 16, 2001, Carlson used the e-mail address of Greg Dubrow, a man with whom he had disagreements in conversations on an internet bulletin board. Carlson sent over 5,000 e-mails from Dubrow's address to a Phillies address, as well as thousands of e-mails to other addresses, from which Dubrow received 6,000 returned e-mails. (JA 2.113; Supp. App. 44, 137-8). On November 19, 2001, Carlson spoofed the e-mail address of Paul Hagen, a sports writer at the Philadelphia Daily News, which caused 6,638 copies of this e-mail to be returned to Paul Hagen's e-mail inbox. (JA, 1.125-127, 3.27-56; Supp. App., 43, 135, 136). On April 9, 2002, Carlson sent thousands of e-mails from an address of a man who he claimed "stalked" him on the internet, 7,000 of which were returned as undeliverable to the alleged stalker's inbox. (JA 2.78-82).

At trial, Carlson admitted to engaging in these activities, but denied that he knew that each time he employed the "indirect attack" method of e-mailing, it would result in a spoofed e-mailer's receipt of hundreds of returned e-mails.[7] (JA 3.176-77). He also denied intending to cause damage by sending thousands of e-mails to one e-mail address,

---

[6] The collection of large lists of e-mail addresses for use in spam or bulk mailing is referred to as "harvesting."

[7] Carlson obtained many e-mail addresses from the unsecured networks of high school and college alumni websites. Because the e-mail addresses of students typically become invalid after they graduate, such websites contain a large number of invalid addresses. Carlson claims he did not consider this result.

which would clog the address, result in delays, and at times require the purging of all e-mails, causing valuable business-related e-mails to be permanently lost.[8]

The present appeal centers around whether the jury's conviction of Mr. Carlson based upon the finding that he intended to cause damage when he sent e-mails, using both direct and indirect attacks, was supported by the evidence.

III.

We must view the sufficiency of the evidence claim[9] in the light most favorable to the Government, *Wolfe,* 245 F.3d at 261, and should sustain a verdict if "any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt*."* *United States v. Dent*, 149 F.3d 180, 187 (3d Cir. 1998) (quoting *United States v. Voigt*, 89 F.3d 1050,1080 (3d Cir. 1996)). A court, however, "must be ever vigilant in the context of Fed. R. Crim. P. 29 not to usurp the role of the jury by weighing credibility and assigning weight to the evidence, or by substituting its judgment for that of the jury." *Flores*, 454 F.3d at 154. Accordingly, an appellant bears a "very heavy burden" to prove the evidence

---

[8] For example, on August 4, 2002, Carlson sent thousands of e-mails from the e-mail address of the vice president of public relations at Knight-Ridder, PNI's parent company, which resulted in the return of 12,000 e-mail messages. Carlson engaged in a similar activity on August 14, 2002. However on this occasion the e-mails were sent from the address of Knight-Ridder's president. The number of returned e-mails was so large that the company had to shut down its server and rid it of all pending e-mails. (JA 2.56-65).

[9] Carlson properly preserved his argument of insufficiency of evidence for appeal by moving for a judgment of acquittal at the conclusion of the evidence. *United States v. Wolfe*, 245 F.3d 257, 261 (3d Cir. 2001).

presented was insufficient to support the verdict. *United States v. Gonzalez*, 918 F.2d 1129, 1132 (3d Cir. 1990) (quoting *United States v. Losada,* 674 F.2d 167, 173 (2d Cir. 1982)).

The Computer Fraud and Abuse Act requires proof that a criminal defendant:

> knowingly cause[d] the transmission of a program, information, code, or command, and as a result of such conduct, ***intentionally*** cause[d] damage without authorization, to a protected computer.

18 U.S.C. § 1030(a)(5)(A)(I)(emphasis added). Section 1030(e)(8) defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." Although the statute itself does not define "intentionally," this Court has defined it in the criminal context as performing an act deliberately and not by accident. *United States v. Barbosa*, 271 F.3d 438 (3d Cir. 2001). Accordingly, the Government was required to prove at trial that Carlson deliberately caused an impairment to the integrity or availability of data, a program, a system, or information.

The jury, after being properly charged as to both the elements of the crime and the definitions of relevant terms used therein, found that Carlson knowingly accessed a computer without authorization and intentionally caused damage thereto. Significantly, the District Court defined the meaning of intent as follows:

> A person acts intentionally when what happens was the defendant's conscious objective. To act intentionally means to do an act deliberately and not by accident. The ultimate fact of intent, though subjective, may be established by circumstantial evidence based upon a person's outward manifestations, his words, his conduct, his acts and all the surrounding circumstances disclosed by the evidence and the rational and logical inferences that may be drawn from them. To find the defendant guilty of Counts 1 through 26, you

> must find beyond a reasonable doubt that he intended to cause damage to the protected computer.

(JA 4.16, 9-19).

At trial, Carlson admitted that in using the direct e-mailing method and sending thousands of e-mails to one inbox, the targeted inbox would flood with e-mails and thus impair the user's ability to access his other "good" e-mails. (JA 3.164-65). Carlson argued, however, that he only believed the targeted e-mail user's ability to access his e-mail would be impaired for a few minutes.

Carlson contended that, in employing the indirect e-mailing method, although he intentionally spoofed e-mail addresses from which he sent thousands of e-mails at a time, he did not intend that the consequence of this would be to flood the spoofed sender's mailboxes with mail that was returned to sender and with replies requesting that the sender not e-mail the recipient in the future. (Appellant's Brief, 2).

The testimony reflected, however, that Carlson was a sophisticated internet and e-mail user. Carlson himself admitted to extensive knowledge of use of the internet and software, including knowledge of how to harvest e-mail addresses from websites, to send mass mailings, to use proxy servers, and to spoof e-mail addresses. (JA 3.151-156, 3.176-177). It is clear from the evidence that Carlson's level of internet savvy, combined with his actions, could rationally be used as circumstantial evidence to conclude that Carlson intended the consequences of his actions.

IV.

We hold that sufficient evidence was presented at trial such that a reasonable juror could have found that Carlson, who intentionally accessed a computer without authorization, also intended the resultant damage. The Judgment of Conviction is affirmed.