IN THE

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. BRET McDANEL, Defendant-Appellant.	C.A. No. 03-50135 D.C. No. CR 01-638-LGB (Central Dist. Cal.) GOVERNMENT'S MOTION FOR REVERSAL OF CONVICTION; MEMORANDUM OF POINTS AND AUTHORITIES; DECLARATION OF RONALD L. CHENG

Plaintiff-Appellee United States of America, pursuant to Federal Rule of Appellate Procedure 27, and by and through its attorney of record, Assistant United States Attorney Ronald L. Cheng, hereby respectfully requests this Court to reverse defendant's conviction in this case. Defendant has served his term of imprisonment and is currently serving his term of supervised release.

//

//

//

//

//

//

//

//

This motion is based upon the files and records of this case, the attached memorandum of points and authorities and the attached declaration of Ronald L. Cheng.

Dated: October 14, 2003

Respectfully submitted,

DEBRA W. YANG
United States Attorney

STEVEN D. CLYMER
Special Assistant U.S. Attorney
Chief, Criminal Division

RONALD L. CHENG
Assistant United States Attorney
Chief, Criminal Appeals Section

Attorneys for Plaintiff-Appellee
UNITED STATES OF AMERICA

MEMORANDUM OF POINTS AND AUTHORITIES

I

INTRODUCTION

Defendant-appellant Bret McDanel has appealed his conviction after court trial (before the Hon. Lourdes G. Baird, United States District Judge) on one count of causing damage to a protected computer, under former 18 U.S.C. § 1030(a)(5)(A) (2000) ("Section 1030"). Among his claims, defendant asserts that the statute of conviction, which requires that one intend to "damage" in the sense of "impairment to the integrity" of a protected computer, does not extend to his conduct, in which defendant transmitted information concerning a means of accessing a computer system to the computer system's users. After further review of this matter in light of the arguments made by defendant on appeal, the government concedes that the evidence did not establish an intent to "damage" within the meaning of the statute, and requests that this Court reverse defendant's conviction.

II

FACTUAL BACKGROUND

Defendant was a systems administrator at Tornado Development, Inc. ("Tornado"). Tornado provided a "unified messaging" service to its customers, which included accounts that held e-mail, voice mail, paging, and faxing services in one place. (Reporter's Transcript ("RT") [6/11/02] 101; Defendant's

Excerpts of Record ("ER") 155). As the company's systems administrator, defendant understood how to test the limits of the system by sending large numbers of e-mail through it to cause it to "crash." In addition, defendant learned that, when a user logged onto the system, the Tornado system would provide a numerical code, known as the "NID," which allowed a user to remain on the system. (RT [6/11/02] 103-13; ER 157-67). If, however, the user linked to an outside website through an e-mail, the Tornado system would transmit the NID to that site and an outsider could theoretically gain access to the user's account through the NID. (Trial Exhibit ("Ex.") 147; RT [6/18/02] 116; ER 288, 545-47). No one had actually broken into the Tornado system through the NID, and the existence of the NID was confidential. (RT [6/11/02] 115, 116; ER 169, 170). As a systems administrator, defendant told Tornado he believed the NID disclosure problem should be fixed, but Tornado declined to do so. (Ex. 19; ER 517-19).

Because of difficulties defendant had with other employees, defendant left Tornado. Afterwards, defendant sent three e-mail attacks between August 31, 2000, and September 5, 2000, through Tornado's server to the company's customers. (RT [6/12/02] 45-48, 76, 90-92; RT [6/14/02] 132-36; ER 175-78, 181, 182-84, 251-55). The volume of e-mails overloaded the capacity of the server and caused the Tornado system to "crash," so that the system was

inoperable until technicians could bring the system back on line. (Id.). Each e-mail, which included a link to a website that defendant operated, informed the reader about the existence and operation of the NID, which defendant characterized as a security flaw that Tornado declined to repair. (Exs. 30-31; ER 520-22).

III

AFTER REVIEW OF THIS MATTER, THE GOVERNMENT CONCEDES THAT DEFENDANT'S CONVICTION SHOULD BE REVERSED

In the district court, the government argued, and the court found, that the evidence supported a conviction for a single violation of § 1030(a)(5). Upon further consideration, in light of arguments presented by defendant on appeal, the government has concluded that these contentions, which the government believed at the time of trial were a proper, good faith construction of the statute, led the district court into error. The government now acknowledges that the evidence adduced below was insufficient to support a finding beyond a reasonable doubt that defendant intentionally caused "damage" to Tornado's computer system (within the meaning of § 1030(a)(5)) that resulted in $5,000 in loss. Accordingly, the government asks that this Court reverse the judgment of conviction entered against defendant.

Section 1030(a)(5), as it existed in 2000, penalizes one who "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 . . . ." The government argued below that defendant's transmission of over 5,000 electronic mail messages to Tornado's customers on September 1, 2000, caused "damage" to Tornado's computer system. As the term "damage" was defined in 18 U.S.C. § 1030(e)(8) (2000), "any impairment to the integrity or availability of data, a program, a system, or information" that causes loss aggregating $5,000 in value to one or more individuals constituted "damage."[1]

The government argued that defendant intentionally caused damage under two theories, both of which were necessary to support the guilty verdict on this charge. The government argued, first, that defendant intentionally caused damage to Tornado's computer system by impairing its availability, in that McDanel knowingly and intentionally sent a sufficient number of messages to cause Tornado's messaging system to overload and fail, and that he intended to have it so fail. All elements under this theory were proven before the district court. This first theory of the case was supported by the evidence, but the total loss connected to the impairment of availability was insufficient by itself to meet the $5,000 threshold required by the statute.

---

[1] The statute permits proof of consequences other than $5,000 in monetary loss to meet this element. 18 U.S.C. § 1030(e)(8)(A)-(D) (2000). The monetary loss element was the only one attempted to be proven at trial, however, and is the only one arguably applicable to this case.

The government also argued that defendant's transmission of electronic mail messages had intentionally caused damage to Tornado's computer system by impairing its integrity, based on the government's good faith belief at the time of trial that a valid interpretation of the statute supported this meaning of "damage." The government now acknowledges that the evidence introduced was insufficient to meet the elements of the statute beyond a reasonable doubt as to this second theory. Without the monetary loss attributable to this second theory, the necessary $5,000 threshold required by the statute cannot be proven, and thus all elements of the charged offense were not proven beyond a reasonable doubt.

In the district court, the government advanced the theory that defendant had intentionally "impaired the integrity" of Tornado's computer system by revealing confidential information relating to the operation of the Tornado server. This information made it easier for outsiders to access this system. It also required Tornado's staff to undertake immediate and expensive corrective action to counteract defendant's actions. These corrective actions included changing Tornado's messaging system so that the vulnerability identified by defendant was patched, testing the system, and consulting with customers concerned that their data may have been accessible. Because Tornado expended significant resources to respond to defendant's

conduct, the government argued that the $5,000 damage threshold had been met.

On further review, in light of defendant's arguments on appeal, the government believes it was error to argue that defendant intended an "impairment" to the integrity of Tornado's computer system. Despite defendant's actions to transmit and publish the vulnerability to Tornado's customers, and the harm to Tornado's business that resulted, there was no proof that defendant intended his messages to aid others in accessing or changing the system or data.[2] Instead, the evidence established that defendant informed Tornado's customers -- the people whose data may have been vulnerable to unauthorized access -- about the vulnerability, an action that could have brought about repair of the problem. Accordingly, because the government did not prove that there was an intent to "impair the integrity" of the computer system in the sense set forth above, the loss directly resulting from the disclosure of the vulnerability itself should not have been attributed to defendant.[3]

---

[2] The government did not argue or seek to prove in the district court that anyone outside of Tornado acted on defendant's message to actually access or change Tornado's system or data. Title 18, United States Code, Section 1030(a)(5), requires that a defendant knowingly cause the transmission of a program, information, code or command, and that intentional damage occur "as a result of" that conduct.

[3] Defendant's actions were not wholly blameless, particularly when viewed in light of the Rule 404(b) evidence admitted relating to his intrusion activity at his former

Defendant's release of vulnerability information did not by itself cause an "impairment to the integrity" of a computer system where there is no proof that "data, a program, a system, or information" has been accessed or changed as a result of that release of information nor that defendant intended such an outcome. It is on this principle that the government confesses error in this case. While distribution of this information with specific intent that someone use it to access or damage a computer system could potentially be illegal, that case is not presented here.

---

employer in New Jersey. Defendant revealed confidential information relating to the operation of Tornado's system and undertook these actions with at least the partial intent to embarrass Tornado and harm its relationship with its customers, as well as to crash its computers, thus disrupting the services it provided. The public revelation of this vulnerability increased the likelihood that someone would access the private correspondence of Tornado's customers. If defendant's specific intent to bring about such a harm to Tornado or its customers had been proven, his conduct might have violated Section 1030 or constituted another crime. For example, knowingly trafficking in "passwords or similar information through which a computer may be accessed without authorization" violates 18 U.S.C. § 1030(a)(6). If defendant had specifically intended that his release of vulnerability information would aid another in committing an intrusion into or damage to Tornado's computers, it could constitute aiding and abetting a violation or an attempted violation of 18 U.S.C. § 1030. An individual could also pass on vulnerability information to another in furtherance of a conspiracy to commit a violation of 18 U.S.C. § 1030 or another crime. Similarly, if an employee reveals confidential business information for profit or with the purpose of defrauding an employer, that conduct could potentially form the basis for a mail or wire fraud charge. 18 U.S.C. §§ 1341, 1343. See Carpenter v. United States, 484 U.S. 19 (1987). Defendant was not charged, however, under any of these theories, and the court need not reach these issues in this case.

Accordingly, the government concedes that there was insufficient evidence to prove a violation of 18 U.S.C. § 1030(a)(5)(A) (2000), the sole offense for which defendant was tried.

IV

CONCLUSION

For the reasons stated above, the government requests that this Court reverse the conviction in this case.

DECLARATION OF RONALD L. CHENG

I, RONALD L. CHENG, hereby declare the following:

1. I am an Assistant United States Attorney in the Central District of California and am the Chief of the Criminal Appeals Section in this office. In that capacity, I am coordinating the preparation of the government's response in United States v. Bret McDanel, D.C. No. 01-638-LGB and C.A. No. 03-50135. I have knowledge of the facts set forth herein and, if called as a witness, could and would testify competently thereto.

2. On October 14, 2003, I attempted to contact defense counsel, Jennifer Stisa Granick, Esq. According to Ms. Granick's voicemail message, Ms. Granick is out of the office until October 20, 2003. and spoke with her assistant, Ms. Joanne Newman. In my voicemail message for Ms. Granick and in my conversation with Ms. Newman, I stated that the government would be filing a motion to reverse defendant's conviction.

//

//

3. Defendant has served his term of imprisonment and is currently on supervised release.

I declare under penalty of perjury, pursuant to the laws of the United States, that this declaration is true and correct.

Executed October 14, 2003, Los Angeles, California.

RONALD L. CHENG

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. BRET MCDANEL, Defendant-Appellant.	C.A. No. 03-50135 D.C. No. CR 01-638-LGB (Central Dist. Cal.) DECLARATION OF SERVICE BY MAIL

I, Nancy Johnson, declare:

That I am a citizen of the United States and a resident of Los Angeles County, California; that my business address is 312 North Spring Street, Los Angeles, California 90012; that I am over the age of 18 years, and am not a party to the above-entitled action; that on **October 14, 2003**, I deposited in the United States mail in Los Angeles, California, in the above-entitled action, in an envelope bearing the requisite postage, a copy of: **GOVERNMENT'S MOTION FOR REVERSAL OF CONVICTION; MEMORANDUM OF POINTS AND AUTHORITIES; DECLARATION OF RONALD L. CHENG**

addressed to:

Jennifer Stisa Granick
Center for Internet and Society
Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, California 94305-8610

at the last known address, at which place there is a delivery service by United States mail.

I declare under penalty of perjury that the foregoing is true and correct.

DATED: This **14th** day of **October, 2003.**

Nancy Johnson

NANCY JOHNSON