

4. The students do not intend to give the presentation scheduled for Defcon at any future conference.

5. On August 8, 2008, the students provided the Massachusetts Bay Transportation Authority (“MBTA”) a confidential report containing sensitive information derived from their research. The report disclosed all important aspects of the students’ research into the security of the Boston T fare system, including details that they never intended to make public. This report has now been revealed to the public through the MBTA’s unsealed filings in this case. As a result, the August 9, 2008 temporary restraining order improperly serves to prevent the students from disclosing to the public information that MBTA itself has already made public.

6. As a result of the students’ research and the attention drawn to it by the above-captioned lawsuit, media in Boston and throughout the world are inquiring as to whether the MBTA’s fare system has adequate security. Because of the August 9, 2008 temporary restraining order, the students are unable to participate meaningfully in that debate.

7. Attached hereto as Exhibit A is a true and correct copy of the Department of Justice’s Motion for Reversal of Conviction, Memorandum of Points and Authorities, Declaration of Ronald L. Cheng filed on October 15, 2003 in *United States v. McDanel*, No. 03-50135 (9th Cir. dismissed Dec. 15, 2003).

8. Attached hereto as Exhibit B is a true and correct copy of a letter to the Court from computer science professors and computer scientists concerning the above-captioned case and dated Aug. 11, 2008.

I declare under penalty of perjury of the laws of the State of California that the foregoing

is true and correct to the best of my knowledge and belief. Executed August 12, 2008 in San Francisco, California.

/s/ Marcia Hofmann
Marcia Hofmann

EXHIBIT A

IN THE
UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

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

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.

//
//
//
//
//
//
//
//
//

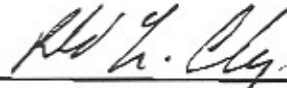
This motion is based upon the files and records of this case, the attached memorandum of points and authorities and the attached declaration of Ronald L. Cheng.

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

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

EXHIBIT B

August 11, 2008

Hon. George A. O'Toole, Jr.
United States District Court
Federal District of Massachusetts
John Joseph Moakley U.S. Courthouse
Courtroom 9, 3rd Floor
1 Courthouse Way
Boston, MA 02210

Re: *Massachusetts Bay Transportation Authority v. Anderson, et. al*,
Case # 08-11364-GAO

**Letter from Computer Science Professors and Computer
Scientists**

Dear Judge O'Toole:

We are computer scientists and researchers, many from the nation's top research and educational institutions. We write in letter form because we understand that time is short and that a temporary restraining order is currently in effect preventing the MIT student researchers from discussing their work. We hope this letter will assist you in your consideration of the Motion for Reconsideration.

Each of us engages in scientific research relating to computer systems and technologies. Each of us also engages in the routine publication and public discussion of that work. Our specific titles are listed with our signatures below.

We were quite troubled to learn that the Court has enjoined the students from discussing their research on the MBTA's fare payment system because that research might materially assist another person in defrauding the system. We write to express our firm belief that research on security vulnerabilities, and the sensible publication of the results of the research, are critical for scientific advancement, public safety and a robust market for secure technologies. Generally speaking, the norm in our field is that researchers take reasonable steps to protect the individuals using the systems studied. We understand that the student researchers took such steps with regard to their research, notably by planning not to present a critical element of a flaw they found. They did this so that their audience would be unable to exploit the security flaws they uncovered. We also believe that restraining orders such as that issued by the court over the weekend could have a devastating chilling effect on such research in the future.

Hon. George A. O'Toole Jr.

August 11, 2008

Page 2

Factual Background to this Letter

The focus of our letter is not on the specifics of this security research done by the MIT student researchers. Instead, we wanted to provide you with information about publishing computer security research and the dangerous impact that restraining orders such as the one issued here could have on that research.

This letter is based on our understanding of the following facts: the MIT students performed security research on the payment mechanisms for the MBTA fare collection system as part of a class project for which they received a superior grade. The students then submitted a presentation based on that research to the DEFCON security conference held in Las Vegas from August 6-10, 2008.

The students presented their research to technical representatives of the MBTA and to the FBI a few days before the conference. They also provided a confidential paper detailing the problems they found and proposed solutions. The confidential paper contained technical information not contained in their planned public presentation. The students informed the MBTA that they were not intending to release the entire results of their research, but instead were intending to withhold key pieces of information that could allow replication of their exploits. We also understand that the students engaged in puffery in advertising their presentation, stating that it would allow "free subway rides for life."

We are aware that both the slides for the intended presentation and the confidential paper have now been made widely publicly available, both through the conference materials submitted prior to the filing of the lawsuit and through filings in the public docket in this case by the MBTA.

The Nature Of Computer Systems Research

Much research in computer systems is based upon analysis - the careful examination of existing systems and approaches in order to understand what works well and what works poorly. Researchers discover flaws. They invent new and improved ways to detect and correct flaws, and they invent new and improved approaches to system design and implementation. This investigative approach has driven the computer systems field forward at an extraordinary pace for more than half a century.

Analysis is no less important when the system being studied is used to pay for public transit or any other public function. The best security systems are not one-off systems designed from scratch for single use, but designs that build upon prior

Hon. George A. O'Toole Jr.

August 11, 2008

Page 3

research. For this reason, it is critical that the researchers and engineers developing new systems be able to study existing ones for advantages and flaws. In turn, a system's ability to withstand repeated attacks best allows engineers and the public to trust its security. At a recent major computer security conference, for instance, about 15% of the papers presented were papers describing attacks on technical systems. Such research is broadly accepted in the profession.

The Importance Of Open Discussion And Publication To Computing Research

Open discussion of computing research and publication of its results is essential to the conduct of computing research. The computing research community is large - many thousands of individuals who follow the literature of security research. In computer science research, the "literature" includes code, algorithms, and their analysis.

Broad review and critique are fundamental to the advancement of research. There is a long history of open research in computer security and information hiding. It is no exaggeration to say that most of the security and information hiding technologies upon which we rely today are the products of this open research process.

The Importance Of Open Discussion And Publication On Public Safety And The Market

The restraining order at issue in this case also fosters a dangerous information imbalance. In this case, for example, it allows the vendors of the technology and the MBTA to claim greater efficacy and security than their products warrant, then use the law to silence those who would reveal the technologies' flaws. In this case, the law gives the public a false sense of security, achieved through law, not technical effectiveness. Preventing researchers from discussing a technology's vulnerabilities does not make them go away - in fact, it may exacerbate them as more people and institutions use and come to rely upon the illusory protection. Yet the commercial purveyors of such technologies often do not want truthful discussions of their products' flaws, and will likely withhold the prior approval or deny researchers access for testing if the law supports that effort.

As an example, computer anti-virus experts rely heavily on public dissemination of timely information about threats on the horizon. For instance, the "Code Red" worm released a few years ago was designed to spread rapidly for about a week, and it was very successful at infecting more than 200,000 computers. Security

Hon. George A. O'Toole Jr.

August 11, 2008

Page 4

researchers across the country rallied together in a concerted effort to blunt the attack, and discovered through last-minute reverse engineering (disassembly) that the worm was designed to make all infected machines attack the White House web server on a specified date. With only a few days to counter this threat, experts were able to study the reverse engineered worm to identify a weakness of the attack and counter it, protecting the White House web server and others. This containment of the Code Red worm would not have been possible without immediate, unrestricted public dissemination of full information about its spread, which included open discussion of the flaws it exposed in other computer software.

Similarly, in 1989 complexity theorists Adi Shamir and Eli Biham invented the technique called differential cryptanalysis, which called into question the strength of various ciphers. The research prevented weaker systems from being adopted to replace the famous DES block cipher, which was then being used by all commercial banking systems and by the U.S. government. Nonetheless, the two scientists were treated as heroes rather than criminals. The publication of a new means of attacking encryption – called differential cryptanalysis - made it possible for the research community to design the AES block cipher, which is vastly more secure as a result of this understanding and is now the federal encryption standard.

This free flow of information also helps the market. With free flow of information about the cost and quality of different payment and security schemes, market forces should lead to the production of better and cheaper schemes. By chilling the flow of information about the quality of competing fare collection schemes, orders such as that issued by the court cripple the market's ability to reward higher quality schemes.

The analogy to the research done by the MIT students is obvious. A break in the security system for payments on the MBTA system teaches how to design better systems. If a break exists it will be discovered. It is much better from everyone's perspective if researchers discover the break and publish it than if unscrupulous discoverers of the break exploit it without public notice. While the publication need not always contain every detail necessary to allow criminal exploitation of the flaw, as the students here rightly decided, the fact of the security flaw should not have been hidden from the public.

Responsible Security Disclosures

It is the case that security researchers need to make careful decisions about how much detail of a particular security break they should make public. Generally

Hon. George A. O'Toole Jr.

August 11, 2008

Page 5

speaking, when large public security systems are at issue, the norm in our field is that researchers take reasonable steps avoid inadvertently teaching others how to exploit the flaw. From what we understand of the facts, the MIT student researchers took such steps in planning their presentation, withholding key information about the flaws they discovered. They also intended to do the same in the future, although this might not be necessary any more since we understand that the MBTA has now voluntarily placed that same information in the public record in this case.

Yet at the same time that researchers need to act responsibly, vendors should not be granted complete control of the publication of such information, as it appears MBTA sought here. As noted above, vendors and users of such technologies often have an incentive to hide the flaws in the system rather than come clean with the public and take the steps necessary to remedy them. Thus, while researchers often refrain from publishing the technical details necessary to exploit the flaw, a legal ban on discussion of security flaws, such as that contained in the temporary restraining order, is especially troubling.

Chilling Effect of the Court's Order

The court's order, if not lifted, will chill research and publication when the technologies or systems in question are used to collect payments on public transportation. Fears of violating vaguely-defined prohibitions are expected to lead researchers to choose "safer" topics of study and to censor their publications rather than risk lawsuits.

In particular, the court's ruling that "transmission" of a computer program to a computer system could include a public presentation about flaws in the security of the system is especially troubling. It is even more so here because we understand that key portions of the research needed to duplicate the attack were not going to be presented at the conference and will not be presented in the future.

Hon. George A. O'Toole Jr.
August 11, 2008
Page 6

Conclusion

In sum, we are concerned that the pall cast by the temporary restraining order will stifle research efforts and weaken academic computing research programs. In turn, we fear the shadow of the law's ambiguities will reduce our ability to contribute to industrial research in security technologies at the heart of our information infrastructure. We urge that you reconsider and remove the temporary restraining order issued on August 10, 2008.

Sincerely,

Professor David Farber¹
Distinguished Career Professor of Computer Science and
Public Policy in the School of Computer Science
Carnegie Mellon University

Professor Steven M. Bellovin
Professor of Computer Science
Columbia University

Professor David Wagner
Associate Professor of Computer Science
University of California at Berkeley

Professor Dan Wallach
Associate Professor of Computer Science
Rice University

Professor Tadayoshi Kohno
Assistant Professor of Computer Science and Engineering
University of Washington

Professor David Touretzky
Research Professor
Computer Science Department &
Center for the Neural Basis of Cognition
Carnegie Mellon University

¹ All titles are for affiliation purposes only.

Hon. George A. O'Toole Jr.
August 11, 2008
Page 7

Patrick McDaniel
Co-Director Systems and Internet
Infrastructure Security Laboratory (SIIS)
Pennsylvania State University

Professor Lorrie Faith Cranor
Associate Professor of Computer Science
and Engineering and Public Policy
Carnegie Mellon University

Professor Matthew Blaze
Associate Professor of Computer and Information Science
University of Pennsylvania

Stefan Savage
Associate Professor
Department of Computer Science and Engineering
University of California, San Diego

Bruce Schneier
Chief Security Technology Officer, BT