UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY Plaintiff v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY Defendants	Civil Action No. 08-11364-GAO Date: August 14, 2008 Time: 11AM

DEFENDANTS ANDERSON, RYAN AND CHIESA'S RESPONSE TO PLAINTIFF'S "MOTION TO MODIFY TERMS BUT NOT DURATION OF TEMPORARY RESTRAINING ORDER" AND CROSS MOTION FOR RECONSIDERATION

INTRODUCTION AND STATEMENT OF FACTS

This motion is about three MIT students' ability to publish academic research applying known theories about security weaknesses to transit fare payment systems used by the MBTA.

On Saturday August 9, 2008, District Judge Douglas P. Woodlock restrained Defendants Anderson, Ryan and Chiesa ("students") from "providing [any] program, information, software code, or command that would assist another in any material way to circumvent or otherwise attack the security of Plaintiff MBTA's fare CharlieTicket and CharlieCard fare collection system." Defendants seek reconsideration of that temporary restraining order on the grounds that (1) the order is an unconstitutional prior restraint on First Amendment protected speech about their academic research, (2) the Computer Fraud and Abuse Act does not prohibit communication of information about computers or computer security, and (3) the MBTA's publication of the defendants' research and presentation slides undermines its claim to injunctive

relief.

Anderson, Ryan and Chiesa study computer security with professor Ronald Rivest at the Massachusetts Institute of Technology. The students applied existing research on stored value cards commonly used for fare payment in transit systems, including the MBTA's CharlieCard and CharlieTicket. This experiment confirmed that an attacker could modify the CharlieCard and CharlieTicket as the existing research predicted, and showed that additional security measures employed by plaintiff Massachusetts Bay Transportation Authority ("MBTA") were inadequate to prevent these modifications. The students wrote a paper for Rivest on their findings and received an "A." They also were accepted to present their research at the DEFCON computer security conference on August 10, 2008 in Las Vegas, Nevada.

The students and the MBTA attempted to contact each other before the DEFCON presentation. The parties set a meeting on August 4, 2008. The MBTA sent Sergeant Detective Richard Sullivan of the MBTA Police, and he brought a special agent from the Federal Bureau of Investigation with him. The students discussed their research with Sullivan and the FBI agent. At the end of the meeting, the understanding was that the students would deliver a short confidential report to the MBTA summarizing their findings and recommendations. The students did in fact deliver that report as planned and believed in good faith that they had satisfied all of the MBTA's requests.

Detective Sullivan submitted a declaration in this case, but his declaration is oddly silent on what the students discussed at that meeting and what the parties' agreement was. Detective Sullivan's declaration does not acknowledge that, as a result of the August 4 meeting, the students were unaware that MBTA had further demands until the afternoon of Friday, August 8 when the MBTA filed this lawsuit.

On the afternoon the suit was filed, and after the students had left Massachusetts for Nevada, MBTA appeared *ex parte* before Judge Woodlock, who was the duty judge. Judge Woodlock then convened a special court session on Saturday morning to hear this matter. The hearing was audio recorded. Counsel for the students, who were not notified about the hearing until after close of business on Friday afternoon, appeared via telephone.

According to counsel's notes, the Court found that 18 U.S.C. § 1030(a)(5)(A) of the Computer Fraud and Abuse Act prohibits the transmission of information to conference attendees or other individuals or groups if that transmission potentially causes damage to a protected computer. The Court also rejected the students' assertion that any restraining order would be an unconstitutional prior restraint on First Amendment protected speech. The court then enjoined and restrained the students "from providing program, information, software code, or command that would assist another in any material way to circumvent or otherwise attack the security of the Fare Media System. [sic]" *Order* at p. 2. The temporary restraining order ("TRO") runs for ten days. Federal Rule Civil Procedure 65(b)(2). As a result of the temporary restraining order the students did not give their presentation at DEFCON and have refrained from commenting on the substance of their research. While the students are no longer able to present their talk at the security conference, and have no plans to present the DEFCON talk in other forums, they wish to publish detailed information concerning the security vulnerability uncovered by their research to an interested public.

On August 11, 2008, after the date for the presentation had passed and after defendants had informed them that they were planning to seek reconsideration of the restraining order, Plaintiff MBTA filed a "Motion to Modify Terms but not Duration of TRO". The requested modification attempts to narrow the current TRO by inserting the phrase "non-public" between

"providing" and "program …" so that it would enjoin defendants "from providing program, non-public information, software code, or command that would assist another in any material way to circumvent or otherwise attack the security of the Fare Media System. [sic]"

STANDARD FOR GRANTING A MOTION FOR RECONSIDERATION

The TRO was granted pursuant to Fed. R. Civ. P. 65. As such, the MBTA was required the demonstrate (and the Court was required to find):

> (1) a substantial likelihood of success on the merits, (2) a significant risk of irreparable harm if the injunction is withheld, (3) a favorable balance of hardships, and (4) a fit (or lack of friction) between the injunction and the public interest.

Nieves-Márquez v. Puerto Rico, 353 F.3d 108, 120 (1st Cir. 2003) (citation omitted). An "[i]njunction is an equitable remedy which should not be lightly indulged in, but used sparingly and only in a clear and plain case." *Plain Dealer Publishing Co. v. Cleveland Type. Union # 53*, 520 F.2d 1220, 1230 (6th Cir. 1975), *cert. den*. 428 U.S. 909 (1977). "The reluctance to exercise this drastic power should be especially great where temporary relief is sought." *Kass v. Arden-Mayfair, Inc*., 431 F. Supp. 1037, 1047 (C.D. Cal. 1977).

A court may grant a motion for reconsideration when the court has misunderstood a party or there is a significant change in the law or facts since the submission of the issues to the court by the parties. *Reyes Canada v. Rey Hernandez*, 224 F.R.D. 46, 48 (D.P.R.2004) (citing *Bank of Waunakee v. Rochester Cheese Sales, Inc.*, 906 F.2d 1185, 1191 (7th Cir.1990)). Under Fed.R.Civ.P. 59(e), a party may direct the district court's attention to newly discovered material evidence or a manifest error of law or fact enabling the court to correct its own errors. *Aybar v. Crispin-Reyes*, 118 F.3d 10, 15 (1st Cir. 1997).

In this motion for reconsideration, the students draw the Court's attention to the following changed facts and manifest errors of law. First, the DEFCON conference at which the students planned to present their research has now passed and the students did not give their talk. They no longer plan to present that talk, but merely want to publicly explain and verify the

security vulnerability uncovered by their research. Second, most, if not all, of the significant facts known to the students about the Fare Media System are now public, either because they are contained in the slides prepared for and distributed at DEFCON before the TRO issued, or because the MBTA filed research information provided to it by the students on the public docket in this case.

Additionally, the court was wrong to give legal weight to MBTA's version of "responsible disclosure". *See* Memo. ISO Plaintiff's Motion for TRO (Dkt. No. 3) at pp. iv-vi. (arguing for a court order enforcing MBTA's view of responsible disclosure). Contrary to the MBTA's arguments, "responsible disclosure" means only that security professionals must carefully consider when and how to disclose vulnerability information. The "responsible disclosure" norm is not to withhold all details until the vendor or insecure party has a chance to fix, but to take reasonable steps to avoid inadvertently teaching others how to exploit the flaw. See Declaration of Marcia Hofmann (hereafter "Hofmann Decl."), Exhibit A, *Letter From Computer Science Professors and Computer Scientists* at 4-5. Withholding key information about the flaws one discovers while publishing other information, as the students here did, is responsible. This is because disclosure can help security as much or more than hurt it, under certain circumstances. See, e.g. Swire, Peter P., *A Model for When Disclosure Helps Security: What is Different About Computer and Network Security?* Journal on Telecommunications and High Technology Law, Vol. 2, 2004. Available at SSRN: http://ssrn.com/abstract=531782.

The students also base this motion on two manifest errors of law – the holding that the CFAA prohibits the communication of information about security problems with computers to any person and the holding that the TRO strikes an acceptable balance between MBTA's financial interests and the students' constitutionally protected speech. The "likelihood of success is the touchstone of the preliminary injunction inquiry." *Philip Morris, Inc. v. Harshbarger*, 159 F.3d 670, 674 (1st Cir. 1998). As discussed in detail below, these manifest errors in law show that the MBTA was never likely to succeed on the merits.

The First Circuit does "not find irreparable injury where only money is at stake and where the plaintiff has a satisfactory remedy at law to recover the money at issue." *Foxboro Co. v. Arabian American Oil Co*., 805 F.2d 34, 36 (1st Cir. 1986). Even a claim of irreparable injury based on an assertion that damages is "not readily susceptible of calculation and likely would not be recovered from the defendants;" *Public Service Co. of New Hampshire v. Town of West Newbury*, 835 F.2d 380, 382 (1st Cir. 1987), is to be closely scrutinized, and "[s]peculative injury does not constitute a showing of irreparable harm." *Id*. at 383.

The MBTA's argument on irreparable harm focuses on trade secret law. *See* Memo. ISO Plaintiff's Motion for TRO (Dkt. No. 3) at pp. iv. This is inapposite. As an initial matter, the MBTA has made no trade secret claim. *See generally* Complaint. Second, trade secrecy law does not protect against reverse engineering, which is all that is claimed here. *See e.g.* Complaint at ¶ 37; *see generally Baystate Technologies, Inc. v. Bentley Systems, Inc*., 946 F.Supp. 1079, 1090-1091 (D.Mass. 1996); *Kewanee Oil Co. v. Bicron Corp*., 416 U.S. 470 (1974) (holding that reverse engineering is a "fair and honest means" to obtain a trade secret).

Instead the potential harm that MBTA fears is only economic – the possibility that someone might learn from the student's research sufficient information to evade fare payment. Moreover, it is very speculative, since the students have repeated told the MBTA that the students never intended to disclose key details in the public presentation. MBTA admits, as it must, that the "MIT Undergrads stated that they did not intend to harm the MBTA." Complaint at ¶ 50. As noted by security professional Eric Johanson, "key information needed to compromise both the Charlie Ticket and the Charlie Card is not present in the Slides." Johanson Decl. (Dkt. No. 14) at ¶ 11. For example, "[t]he Slides depict a field called 'checksum,' and show that it changes when the ticket value changes, but do not describe how to compute the checksum." *Id*. at ¶ 23; *see also* Confidential Vulnerability Report ("CVR") filed as Henderson Decl. Exhibit 1 (Dkt. No. 10-1) at 2 ("We have purposefully omitted details of this checksum in any public disclosures...").

To the extent that the MBTA has increased the risk of harm by filing the CVR in the public docket, it should not be able to place responsibility on the students.

The balance of hardships also favors the students. When a court balances the hardships, it "must be concerned not only with possible injury to a plaintiff but also with possible injury to the defendant." *Everett J. Prescott, Inc. v. Ross*, 383 F. Supp. 2d 180, 191 (D. Me. 2005). "The loss of first amendment freedoms, for even minimal periods of time, unquestionably constitutes irreparable injury." *Elrod v. Burns*, 427 U.S. 347, 373 (1976) (plurality opinion of Brennan, J.).

As noted in the Complaint, the "MIT Undergrads [were] scheduled to give their 'The Anatomy of a Subway Hack' presentation at 1:00 on Sunday, August 10, 2008." Complaint at ¶ 47 (Dkt. No. 1). The conference is now over, the students were silenced, and the presentation will never be given. Hofmann Decl. at ¶¶ 3-4. Even though the Defcon conference is over, the students remain enjoined from disclosing the fruits of their security research, or otherwise demonstrating the security flaws in the MBTA's systems. This restriction causes the students great hardship.

On Monday, August 11, the MBTA filed a motion which raised the question of "whether this is in fact a 'prank,' or whether the MIT Undergrads are in fact able to compromise the Fare Media System in the manner they publicly claim." Motion to Modify Terms But Not Duration of Temporary Restraining Order at 3 (Docket No.16). Likewise, on August 12, the MBTA said to the *Boston Globe*:

> "There have been claims in the past that have been made against our card or other cards, and, happily, they've all been able to be dismissed or dealt with," said Daniel A. Grabauskas, general manager of the Massachusetts Bay Transportation Authority. "I'm confident it will be the same thing here."

Christopher Baxter & Hiawatha Bray, *MIT students' report makes security recommendations to T*, *Boston Globe* (August 12, 2008). Thus, the MBTA is publicly questioning whether the reports that the transit agency is not sufficiently secure are true. The students' research has raised valid concerns about the security of the MBTA's stored value cards, and the students reject the

notion that their research was nothing more than a "prank." However, under the terms of the TRO, the students are unable to effectively participate in this public debate.

Likewise, the public interest strongly favors disclosure. "The public interest carries considerable weight in these matters. … The court must weigh any hindrance or furtherance of the public interest likely to result from interim injunctive relief." *Sheck v. Baileyville School Committee*, 530 F. Supp. 679, 693 (D. Me. 1982) (citing *Yakus v. United States*, 321 U.S. 414, 440-41 (1944)). "Protecting rights to free speech is *ipso facto* in the interest of the general public." *Westfield High School L.I.F.E. Club v. City of Westfield*, 249 F. Supp. 2d 98, 128 (D. Mass. 2003) (citing *Machesky v. Bizzell*, 414 F.2d 283, 289 (5th Cir. 1969) ("First Amendment rights are not private rights ... so much as they are rights of the general public.")).

As an initial matter, open discussion of security vulnerabilities is in the public interest:

> Although presentations on security vulnerabilities often discuss how weaknesses might be exploited, prohibition of open discussion and publication of security vulnerabilities greatly harms the ability of researchers to function, and has a chilling effect not only on publication, but on whether some important research is done in the first place, greatly stifling scientific advancement.

Johanson Decl. (Dkt. No. 14) at ¶ 16; *see generally id.* at ¶¶ 12-18.

Moreover the question of whether or not the MBTA, "a political subdivision of the commonwealth," MGL § 161A-2, is adequately performing its public services remains clouded. Media from Boston and all over the world are now inquiring as to whether the MBTA has adequate security. Hofmann Decl. at ¶ 6. Again the students are unable to participate meaningfully in that debate. *Id.*

It is in the public interest for the residents of the commonwealth to know truthful information about the performance of the security operations of a political subdivision of the commonwealth, which is subsidized by billions in public funds. *See* Complaint at ¶ 19-20 (detailing the billions of tax dollars MBTA received since the 1960s); *see also News Group Boston, Inc. v. National R.R. Passenger Corp.*, 799 F. Supp. 1264 (D. Mass. 1992) (recognizing public interest in opening the operations of a quasi-government transportation agency to the

scrutiny of the public and allowing oversight of operations of a company which is subsidized by taxpayer monies).

I. THE COMPUTER FRAUD AND ABUSE ACT PROHIBITS THE TRANSMISSION OF INFORMATION OR CODE TO A PROTECTED COMPUTER THAT HARMS THAT COMPUTER, NOT THE COMMUNICATION OR DELIVERY OF NON-CLASSIFIED INFORMATION OR CODE TO ANY PERSON OR PERSONS

The Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(5)(A), is a criminal statute targeting unauthorized access to computers, and not the communication of information to other individuals, as Judge Woodlock has held. This is based on five arguments.

First, the text of the section indicates--by the placement of a comma before the clause "to a protected computer"--that the offender must both transmit information to the protected computer and cause damage to that same computer. An offender must transmit information to and harm a protected computer, not to another person, to violate section 1030(a)(5)(A). That section reads:

> Whoever … 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; and [causes or would have caused certain specified loss or harm] shall be punished as provided in subsection (c) of this section.

18 U.S.C. § 1030(a)(5)(A). If possible, the Court must "'give effect ... to every clause and word of a statute.'" *See Duncan v. Walker*, 533 U.S. 167, 174 (2001) (*quoting United States v. Menasche*, 348 U.S. 528, 538-39 (1955)). There is a comma between the word "authorization" and the clause "to a protected computer." That comma indicates that "to a protected computer" modifies both the preceding clauses. Both the transmission and the damage must be to a protected computer.

Second, the plain language of the statute indicates that "transmission of information" does not mean "communication of information." This is most easily seen by comparison to

section 1030(a)(1) , which expressly includes a prohibition on "communication" of information about computers deemed to be protected for national defense and related specific purposes.

Section 1030(a)(1) states that:

> Whoever— having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained [Government classified] information … with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully **communicates, delivers,** transmits, or causes to be **communicated**, **delivered**, or transmitted, or attempts to **communicate**, **deliver**, transmit or cause to be **communicated**, **delivered**, or transmitted the same **to any person** not entitled to receive it … shall be punished as provided in subsection (c) of this section.

(Emphasis added.). Where Congress intended to prohibit the dissemination of information to other persons, it clearly indicated so with specific language to that effect. It did not do so in section 1030(a)(5)(A) relied on by the plaintiffs here.

Thus, as the statute itself makes clear, when Congress seeks to control the dissemination of information, it uses the words "communicate" and "deliver" in addition to "transmit," and specifies that the information it seeks to control may not be given "to any person" not entitled to receive it. These phrases are not included in section 1030(a)(5)(A), showing that that section does not apply to or regulate the dissemination of information to persons.

Third, the legislative history of the CFAA shows that Congress intended "transmission" as a technological term used to refer to sending digital programs, software, code or information to a computer. ""Transmission does not refer speech or other forms of communication to human beings. *See* The Introduction of the National Information Infrastructure Protection Act, 104th Congress (1996) (Statement of Hon. Bob. Goodlatte in the House of Representatives) (The provision at issue here "would . . . penalize any person who uses a computer to cause the transmission of a computer virus or other harmful computer program to Government and financial institution computers."). This interpretation has been confirmed by the United States in a criminal prosecution under the statute. See *Government's Motion for Reversal of Conviction, Memorandum of Points and Authorities, Declaration of Ronald L. Cheng,* filed in *United States*

v. McDanel, Ninth Circuit Court of Appeals No. 03-50135 and attached as Exhibit B to the Hofmann Decl.

Because the Court misread section 1030, there is no legal basis for the TRO, which was expressly based only on that provision. For this reason, the order was erroneously entered and should be dissolved. Furthermore, to the extent that the CFAA provision is read to allow the prior restraint of communication of truthful information to people-- as distinguished from transmission from one computer that harms another -- the statute would be in tension with the First Amendment. As such, the doctrine of constitutional avoidance should lead the court to adopt an interpretation of the CFAA that does not raise questions about whether the statute impermissibly burdens First Amendment-protected speech.

The legislative history of the CFAA shows that Congress intended "transmission" as a technological term used for sending digital programs, software, code or information to a computer, and not including speech to other human beings. Until 1994, the CFAA generally prohibited unauthorized access to computers. By that point, however, Congress had become familiar with the problem of computer viruses that damage computers but do not give a trespasser unauthorized access. As such, the statute was amended to include a prohibition on damaging computers through unlawful transmissions of viruses from one computer to another. *See* 18 U.S.C. § 1030(a)(5) (1994). As Senator Leahy explained:

> [C]omputer abusers have developed an arsenal of new techniques which result in the replication and transmission of destructive programs or codes that inflict damage upon remote computers to which the violator never gained "access" in the commonly understood sense of that term. The new subsection of the CFAA created by this bill places the focus on harmful intent and resultant harm, rather than on the technical concept of computer "access."

Violent Crime and Control and Law Enforcement Act of 1994 - Conference Report, 103rd Cong. (1994) (Statement of Sen. Leahy).

In 1996, Congress adjusted the 1994 provisions to the language we see in section 1030(a)(5)(A) today. The legislative history shows that Congress intended the provision to prohibit damaging transmissions of computer viruses and the like from one computer to another:

> The bill would also penalize any person **who uses a computer** to cause the transmission of a computer virus or other harmful computer **program to Government and financial institution computers** not used in interstate communications, such as intrastate local area networks used by Government agencies that contain sensitive and confidential information.

The Introduction of the National Information Infrastructure Protection Act, 104th Congress (1996) (Statement of Hon. Bob. Goodlatte in the House of Representatives), (emphasis added). The legislative history is further proof that the CFAA does not regulate speech about computers, but attacks on computers, whether through unauthorized access or through computer viruses, "worms" and the like.

"'[I]t is a cardinal principle' of statutory interpretation … that when an Act of Congress raises 'a serious doubt' as to its constitutionality, 'this Court will first ascertain whether a construction of the statute is fairly possible by which the question may be avoided.'" *See, e.g., Zadvydas v. Davis*, 533 U.S. 678, 689 (2001) (*quoting Crowell v. Benson*, 285 U.S. 22, 62 (1932); *Ashwander v. Tennessee Valley Authority*, 297 U.S. 288 (1936) (Brandeis, J., concurring)). To the extent that the CFAA regulates information about computer security flaws, it is a content-based speech regulation, presumptively unconstitutional and subject to strict constitutional scrutiny.

II. THE TEMPORARY RESTRAINING ORDER IS AN UNCONSTITUTIONAL PRIOR RESTRAINT ON PROTECTED SPEECH AND MUST BE OVERTURNED

This TRO is an unconstitutional prior restraint that must be overturned, and no preliminary injunctive relief could constitutionally issue in the alternative. A prior restraint is a government regulation that limits or conditions in advance the exercise of protected First Amendment activity. Prior restraints are extremely disfavored and rarely, if ever, upheld. The Supreme Court has rejected prior restraints in cases involving national security, and cases where

the information to be published has been illegally obtained, whether by a third party or by the speaker. The TRO here, which has already resulted in preventing the students from presenting their research publicly and which continues to gag them from discussing their factual findings, is unjustified, vague and overbroad. It must be rejected and no TRO or other restraining order should issue at least until there has been a full trial on the merits to determine whether the students have (1) committed the alleged torts and (2) whether their conduct or the content of their research means that their research findings are not constitutionally protected.

A judicial injunction that prohibits speech prior to a determination that the speech is unprotected constitutes a prior restraint. *Near v. Minnesota*, 283 U.S. 697, 719 (1931). Any prior restraint is the most dangerous imposition on individuals' freedom of speech. *Nebraska Press Ass'n v. Stuart*, 427 U.S. 539, 559 (1976) ("Prior restraints on speech and publication are the most serious and least tolerable infringement on First Amendment rights"). Therefore, request for such a restraint "comes to [the] Court bearing a heavy presumption against its constitutional validity." *New York Times Co. v. United States*, 403 U.S. 713, 714 (1971). See also *Auburn Police Union v. Carpenter*, 8 F.3d 886, 903 (1st Cir. 1993).

"In the case of a prior restraint on pure speech, the hurdle is substantially higher [than for an ordinary preliminary injunction]: publication must threaten an interest more fundamental than the First Amendment itself. Indeed, the Supreme Court has never upheld a prior restraint, even faced with the competing interest of national security or the Sixth Amendment right to a fair trial." (*Proctor & Gamble Co. v. Bankers Trust Co.*, 78 F.3d 219, 226-227 (6th Cir. 1996); *cf. Nebraska Press Assn. v. Stuart,* 427 U.S. 539, 563 (1976) (the Sixth Amendment right of a criminal defendant to a fair trial does not outrank the First Amendment right of the press to publish information); *New York Times Co. v. United States* (1971) 403 U.S. 713, 718-726 ("national security" interest in suppressing classified information in the Pentagon Papers did not outrank First Amendment right of press to publish classified information). "[I]t is clear that few things, save grave national security concerns, are sufficient to override First Amendment interests." *United States v. Progressive, Inc.* 467 F. Supp. 990, 992 (DC Wisc. 1979) (court

issued prior restraint on publication of technical information about hydrogen bomb only because it found that such information was analogous to information about troop movements which posed a grave threat to national security).

The Plaintiff has not and cannot justify a prior restraint on the speech at issue in this case, as explained below. First, truthful scientific speech, including instructions that enable the recipient to use the scientific information for an illegal purpose, are constitutionally protected.[1] For example, information about how to cultivate marijuana or how to pick a lock is constitutionally protected. Second, the speech remains protected even if the students obtained the information illegally (which they did not) or if another party could use the information for illegal purposes. Third, the information is on a matter of public interest. In contrast, the MBTA's interests do not come close those of the government in the Pentagon Papers case, which also failed to justify a prior restraint on publication.

This TRO limits the exercise of the students' free speech, despite the fact that the First Amendment protects scientific speech. Courts have subjected restrictions on the dissemination of technical scientific information and scientific research to First Amendment scrutiny. *United States v. Progressive, Inc.*, 467 F. Supp. 990 (W.D. Wis. 1979); Board of Trustees of *Stanford University v. Sullivan*, 773 F. Supp. 472, 473 (D.D.C. 1991). Instructions are also constitutionally protected expression. *See*, *e.g.*, *United States v. Raymond*, 228 F.3d 804, 815 (7th Cir. 2000) (First Amendment protects instructions for violating the tax laws, but not where such instructions are an incitement to imminent unlawful activity); *United States v. Dahlstrom*, 713 F.2d 1423, 1428 (9th Cir. 1983) (same); *Herceg v. Hustler Magazine, Inc.*, 814 F.2d 1017, 1020-25 (5th Cir. 1987) (First Amendment protects instructions for engaging in a dangerous sex act); *see also Bernstein v. United States Department of State*, 922 F. Supp. 1426, 1435 (N.D. Cal. 1996) ("Instructions, do- it-yourself manuals, [and] recipes" are all "speech"). Thus the TRO in

[1] Nor do First Amendment protections disappear if the MBTA does not approve of the tone of the speech. As Justice Frankfurter wrote, the right of free expression "means not only informed and responsible criticism but the freedom to speak foolishly and without moderation." *Baumgartner v. United States*, 322 U.S. 665, 674 (1944).

this matter, which continues to prevent the students from publicly discussing scientific facts and research that they have conducted, is an unconstitutional prior restraint.

The TRO as initially granted restricted the students from providing true, publicly known, legally acquired information about the MBTA's CharlieCards and CharlieTickets in violation of the First Amendment. See *Veilleux v. National Broadcasting Co.*, 206 F.3d 92, 127 (1st Cir. 2000) (truthful information is more deserving of protection than false information). The current TRO as the MBTA suggests that it be modified still restricts the students from providing true, legally acquired information about these cards This restriction also violates the First Amendment. *Id. See also Bartnicki v. Vopper*, 532 U.S. 514, 535 (2001) (the publication of even illegally-acquired information enjoys some First Amendment protection).

This conclusion does not change even if other people could use the information contained in the students' presentation for criminal purposes. Settled precedent provides that even such information is constitutionally protected. The Supreme Court has stated that while there are some rare occasions in which a law suppressing one party's speech may be justified by an interest in deterring criminal conduct by another, these occasions are extremely rare, and only occur when the speech at issue is of extremely low value. *Id.* at 530 (referring to child pornography). The speech at issue here is of much higher value than child pornography, consisting of facts learned from scientific investigation and analysis. Most speech that is alleged to be "crime facilitating" has both harmful and valuable uses, including some that are not initially obvious. Eugene Volokh, *Crime-Facilitating Speech*, 57 STAN. L. REV. 1095, 1105 (2005).

For example, the letter from computer science professors and computer scientists discusses the ways in which disclosure of security vulnerability information promotes security rather than defeats it, regardless of the wishes of the entity whose systems are weak. Hofmann Decl. Exhibit A at 2 ("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"); *see also* 5 ("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. … 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.")

Because disclosure can benefit security and because security researchers need to make careful decisions about how much detail about a particular security risk they should make public, prohibiting vulnerability disclosure before any adjudication of criminality or constitutionality is unconstitutional. Recognition that it is hard to judge whether speech is "good" or "bad" ahead of time is the basis for the constitutional distaste for prior restraints.

Even if the information contained in the students' presentation was itself obtained illegally, which it was not, that information is constitutionally protected and my not be the subject of a prior restraint. In *In re King World Productions, Inc.*, 898 F.2d 56 (6th Cir. 1990), the Sixth Circuit overturned a temporary restraining order prohibiting a news program from airing video footage it illegally taped of a doctor allegedly engaging in malpractice. Similarly, in *CBS, Inc. v. Davis*, 510 U.S. 1315 (1994), a television network obtained undercover footage at a South Dakota meat packing plant that it intended to air. The packing plant operator obtained an order restraining the network from broadcasting its footage. The Court vacated the temporary restraining order: "Although the prohibition against prior restraints is by no means absolute, the gagging of publication has been considered acceptable only in 'exceptional circumstances.'" *Id.* at 1317.

These are not exceptional circumstances. The students' research on the MBTA's fare payment system is a matter of great public concern. Even before this case occurred, both the Boston Globe and the Boston Herald published articles on security flaws with the CharlieCard. Bray, Hiawatha, "*T Card Has Security Flaw, Says Researcher*", Boston Globe, March 6, 2008; Szaniszlo, Marie, "*Research: Charlie Card is Far From Hack Proof*", Boston Herald, March 6, 2008. On the other hand, the MBTA's interest in keeping this information quiet is certainly no

greater than that of the government in squelching the Pentagon Papers. Nor is the possibility that someone may use the information to get free subway rides sufficient reason to suppress publication of the research.

Finally, the scope of this TRO is both overbroad and vague. The initial TRO unconstitutionally prohibited discussion even of information the plaintiff placed in the public record. MBTA has moved to narrow the TRO to only "non-public" information in recognition of this problem, but this limitation does not resolve the issue. is the TRO remains vague because it is uncertain what information materially helps another person to circumvent the security of the Fare Media System. As the court stated, merely drawing attention to a security problem could focus an attacker on the fact that a particular attack can be done and might be worth trying. The attacker no longer has to wonder whether it is possible; it is. Just that fact might materially assist someone. It is impossible to know in advance, and neither the court nor MBTA could give any clear guidance, which is why counsel felt compelled to advise the students that they could not give their presentation at the Defcon conference. As the Court itself recognized, red-penciling the student presentation to delete objectionable material was not a viable option, the injunction meant that the students might choose not to go forward with their talk, and that if they did, they faced the possibility of contempt charges. Thus, the TRO chilled protected speech.

///

CONCLUSION

For the foregoing reasons, the students request that this court vacate the temporary restraining order.

DEFENDANTS ANDERSON, RYAN AND CHIESA

By their attorneys,

Dated: August 12, 2008

/s/ Emily A. Berger

Emily A. Berger, BBO No. 650,841
emily@eff.org

Jennifer Stisa Granick, CA Bar No. 168423
Jennifer@eff.org
Kurt Opsahl, CA Bar No. 191303
kurt@eff.org
Marcia Hofmann, CA Bar No. 250087
marcia@eff.org

ELECTRONIC FRONTIER FOUNDATION
454 Shotwell St.
San Francisco, CA 94110
(415) 436-9333
(415) 436-9993 (fax)