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

MEMORANDUM IN SUPPORT OF PLAINTIFF'S MOTION TO CONVERT TEMPORARY RESTRAINING ORDER TO TIME-LIMITED PRELIMINARY INJUNCTION--
LEAVE TO FILE GRANTED ON AUGUST 18, 2008

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

By its attorneys,

Ieuan G. Mahony (BBO #552349)
Maximillian J. Bodoin (BBO # 667240)
HOLLAND & KNIGHT LLP
10 St. James Avenue
Boston, MA 02116
(617) 523-2700

Thomas F.S. Darling III (BBO #558848)
MASSACHUSETTS BAY TRANSPORTATION AUTHORITY
State Transportation Building, 7th Floor
10 Park Plaza
Boston, MA 02116
(617) 222-3174

Dated: August 18, 2008
Boston, Massachusetts

Table of Contents

Introduction

The plaintiff, Massachusetts Bay Transportation Authority ("MBTA"), seeks to convert the existing temporary restraining order (the "TRO"), to a Preliminary Injunction, for a five-month period to allow the MBTA to remedy the vulnerabilities disclosed in the CharlieTicket system.

Procedural Posture

At an emergency hearing session on Saturday, August 9, 2008, the Court issued a Temporary Restraining Order (the "TRO"). This TRO expires as of 1:30 PM eastern time on Tuesday, August 19, 2008

Facts

I. The MBTA's Automated Fare Collection System Relies On CharlieTickets and CharlieCards.

The MBTA's automated fare collection system (the "AFC System" or the "Automated Fare Collection System") relies on so-called CharlieCard passes and CharlieTicket passes for the payment of MBTA fares (among other purposes).[1] The fare media system (the "Fare Media System") contains security features, designed to prevent unauthorized personnel from manipulating the system, and obtaining free MBTA transit services or causing other harm.[2] The Fare Media System is a core component in the overall AFC System, and the procurement and installation of this System cost in excess of $180 million.[3]

II. The MIT Students' Examine Security Vulnerabilities In CharlieTickets And CharlieCards In Connection With Their MIT Coursework; They Receive An "A" On Their Class Paper.

[1] Kelley Decl. [6] ¶¶13-16.

[2] Foster Decl. [5] ¶¶4-5.

[3] Kelley Decl. [6] ¶12.

The MIT Students were enrolled in a course with Professor Rivest, a renowned authority on security and encryption. As part of their coursework, they collected information and prepared a paper concerning security vulnerabilities in the AFC's Fare Media System. The MIT Students, the MBTA understands, received an "A" on this paper (the "Class Paper").[4] This paper, the MBTA understands, formed the basis for the Students' activities with respect to the DEFCON Conference.

III. The DEFCON Conference Is One Of The Oldest And Largest Continuous Hacker Conventions In The World.

According to information published by DEFCON, the DEFCON Conference is "one of the oldest continuous hacker conventions around, and also one of the largest." The DEFCON Conference was scheduled to take place this year at the Riviera Hotel & Casino in Las Vegas, Nevada.[5] Organizers state that the Conference is anticipated to draw 5,000 to 7,000 attendees. According to organizers, "technology and hacking is the *core*" of the Conference.[6] The Conference was scheduled to begin on Friday, August 8, 2008.

IV. As Early May 14, 2008, The MIT Students Began Preparing To Present At The DEFCON Conference.

On May 14, 2008, the defendant, Zach Anderson, made a formal submission seeking to have the MIT Students selected as speakers at the 2008 DEFCON Conference.[7] The submission was entitled "The Anatomy of a Subway Hack: Breaking Crypto RFIDs and Magstripes of Ticketing Systems." In this submission, Anderson stated that he and his team would be

[4] The MIT Students have yet to submit testimony, by declaration or otherwise, and declined to be available for deposition. Accordingly, certain facts within the purview of the MIT Students are based on the MBTA's understanding.

[5] *See* https://www.defcon.org/html/links/dc-faq/dc-faq.html.

[6] *See id.* (emphasis added).

[7] Third Mahony Decl., Ex. 1, at MBTA1-2

"releasing a new tool" and would be providing "several" demonstrations.[8] In the body of the submission, Anderson identified the range of software tools the MIT Students proposed to release at the Conference, and tied each of these tools to a specific target. In addition, Anderson identified the various demonstrations that would take place. Specifically, the submission states:

> III. Our Attacks On The Boston T
> …
> B. MIFARE RFID card attacks (on the CharlieCard)
>
> 1. Using the USRP and GNUradio to sniff raw data [**code release]**
>
> 2. Brute forcing attack on 48-bit key (using FPGAs) [**POSSIBLE demo** and **code release** (possible because as of today, the Verilog is not finished)]
>
> 3. Crafted challenge-response attack
>
> 4. Algebraic attacks [**code release**]
>
> C. MagStripe Card Reverse Engineering and attacks (cloning and forgery attacks) on the CharlieTicket
>
> 1. Reverse engineering the data on the card [**automated magstripe reverse engineering tool release**]
>
> 2. Forging a card (AKA how to get a lot of free money) [**python script release and demo**]
>
> 3. Cheap ways of cloning the card[9]

The presentation thus contained approximately two demonstrations, and upwards of five separate releases of software code or other tools to carry out the referenced "attacks."

In the submission, moreover, Anderson notes that a sample slides, and a "whitepaper" about their activities is available on the web, located on MIT servers.[10] This whitepaper appears to be the Class Paper that the MIT Students have refused to produce in this matter.

---

[8] Id.

[9] Third Mahony Decl., Ex. 1, at MBTA2-3

[10] Id. at MBTA 3-4.

A. The MIT Students Contract To Provide To DEFCON The Software Tools And Other Presentation Materials; They Grant DEFCON And All Attendees Unlimited Rights To Use The Materials For All Purposes.

In connection with this submission, Anderson also entered into a contract with DEFCON, that would become operative if DEFCON selected the MIT Students as speakers.[11] In this contract, the MIT Students granted DEFCON the right and permission to "duplicate, record and redistribute this presentation; including, but not limited to, the conference proceedings, conference CD, video, audio, hand outs(s) to the conference attendees for educational, on-line and *all other purposes*."[12]

In addition, Anderson digitally signed a contract whereby he agreed as follows:

> If I am selected to speak, I … understand that I must complete and fulfill the following requirements or I will forfeit my honorarium: 1) I will submit a completed (and possibly updated) presentation, a copy of the tool(s) and/or code(s), and a reference to all of the tool(s), law(s), Web sites and/or publications referenced to at the end of my talk and as described in this CFP submission for publication on the conference CD by noon PST, June 30, 2008.[13]

The MIT Students, therefore, agreed by contract to provide the software tools, presentation, demonstrations, and other materials specified in their submission. The MIT Students now refuse to produce these software tools, and other materials that accompanied their demonstrations.

B. In Submitting Their Completed Presentation To DEFCON, The MIT Students Make The Materials Publicly Available On The Web, Beginning June 30, 2008.

After being selected as speakers, the MIT Students finalized their presentation materials. The deadline for submission was June 30, 2008 and, by an email of that date, Anderson informed

[11] Id. at MBTA 4-6.

[12] Id. at MBTA 4-5 (emphasis added).

[13] Id. at MBTA 4-5 (emphasis added).

Nikita Caine, DEFCON's "Administrator of Khaos", that the slides were available to download from the web.[14] The fact that no password is included or referenced in this email indicates that the presentation materials were freely available to all.

C. The MIT Students Advertise Their Talk On The Internet By Claiming The Ability To Provide "Free Subway Rides For Life."

On July 30, a vendor responsible for components of the Automated Fare Collection System notified the MBTA of its discovery of an Internet advertisement that advertised a presentation at the upcoming DEFCON 16 "hacking" conference (the "Initial Announcement").[15] The Internet advertisement read, in relevant part, as follows:

> Want free subway rides for life? In this talk we go over weaknesses in common subway fare collection systems. We focus on the Boston T subway, and show how we reverse engineered the data on magstripe card, we present several attacks to completely break the CharlieCard, a MIFARE Classic smartcard used in many subways around the world, and we discuss physical security problems. We will discuss practical brute force attacks using FPGAs and how to use software-radio to read RFID cards. We go over social engineering attacks we executed on employees, and we present a novel new method of hacking WiFi: WARCARTING. We will release several open source tools we wrote to perform these attacks. With live demos, we will demonstrate how we broke these systems.[16]

The Initial Announcement specifically targets the MBTA and its computerized Fare Media systems. The Announcement reads, for example: "[w]e focus *on the Boston T subway,* and show how we reverse engineered the data on *magstripe card* [apparently referring to the CharlieTicket], we present several attacks to completely break *the CharlieCard.*" (emphasis added). The Initial Announcement states that the MIT Students have wholly compromised the CharlieCard system, reading, for example, that " we present several attacks to *completely break*

[14] Third Mahony Decl., Ex. 1, at MBTA10.

[15] Docket No. 20, Ex. 1.

[16] Docket No. 20, Ex. 6.

the CharlieCard." (emphasis added). Moreover, in the Initial Announcement, the MIT Students promise to provide to attendees at their presentation "*free subway rides for life*." Finally, the MIT Students claim that they will provide software tools to allow others to "break" the MBTA's CharlieCard and CharlieTicket system. Specifically, the Initial Announcement states that "[w]e will release *several open source tools* we wrote to perform these attacks. With live demos, *we will demonstrate how we broke these systems*."

Accordingly, the MIT Students promised, in the Initial Announcement, to instruct and enable others to "break" the MBTA's computerized Fare Media system. Although the MIT Students later revised this Initial Announcement, the substance of the message remained unchanged.[17]

V. Law Enforcement Requests A Meeting With The MIT Students; The Students, Professor Rivest, MIT Counsel, And Law Enforcement Meet On August 4, 2008.

After learning of the Initial Announcement, the MBTA sought to schedule a meeting with the MIT Students. When Anderson learned of the MBTA's concerns, he promptly (on July 31) emailed DEFCON to determine whether it might be possible to change some of the information in the MIT Students' presentation materials.[18] DEFCON responded by stating that it was not possible to change the materials, as they had already been burned into CDs. DEFCON gave the MIT Students the option, instead, of canceling their talk.[19] Anderson replied that he thought "we will be alright" because, he said, "[w]e left out a couple of key details from the slides." Anderson told DEFCON to "expect" them to give the talk.[20]

---

[17] *See* Docket No. 20, Ex. 7.

[18] Third Mahony Decl., Ex. 1, at MBTA12-14 ("The MBTA informed us today that the FBI has mounted an investigation regarding the work we are going to present at Defcon about hacking subway systems. If still possible, *we may want to adjust a couple of slides from our slide deck*") (emphasis added).

[19] Third Mahony Decl., Ex. 1, at MBTA12-13.

[20] Third Mahony Decl., Ex. 1, at MBTA12.

A. At Their Request, Professor Rivest Acts On The Students Behalf To Coordinate Communications.

The MIT Students relied on Professor Rivest to schedule the August 4 meeting.[21] Indeed, Sgt. Sullivan worked through Professor Rivest to coordinate the parties, time, locations, and other logistics.[22] Professor Rivest then attended the meeting,[23] further indicating the MIT Students' reliance on him as advisor and agent.

B. At The Meeting, The Students State They Have Engaged In No Illegal Conduct In Preparing Their Materials, And Promise To Make No Sensitive Disclosures.

At this meeting, the MIT Students stated several times that they did not hack into the MBTA's computer system while doing research for their presentation, and that they did not attempt to defraud the MBTA by making counterfeit cards.[24] The MIT Students also assured law enforcement that their presentation was on the MIFARE system and the Magstripe system only, and that they would withhold key elements that would allow others to exploit the vulnerabilities that they claimed to have discovered in the MBTA's CharlieCard System.[25] The MIT Students agreed to provide to law enforcement a paper showing the perceived vulnerabilities in the system, in two weeks.

The MIT Students did not offer to provide Sgt. Sullivan with any documents other than the report in two weeks, and Sgt. Sullivan did not ask for any additional materials.[26] The

---

[21] Docket No. 31, Ex. 1 at 3 ("The students had also been in contact with the MBTA since July 31 *through Ronald L. Rivest*, the professor who had overseen their 6.857 project") (emphasis added).

[22] Sullivan Decl. [4] ¶5.

[23] Sullivan Decl. [4] ¶7.

[24] Supp. Sullivan Decl. [37] ¶4.

[25] Supp. Sullivan Decl. [37] ¶5.

[26] Supp. Sullivan Decl. [37] ¶7.

Students did not tell Sgt. Sullivan and Agent Shaver that they had sent these materials to DEFCON for publication roughly a month earlier.

C. Based On These Assurances, Law Enforcement States That No Illegal Activity Is Present, And Requests A Report of Security Vulnerabilities In Two Weeks.

Based on the MIT Students' statements that they did not hack into the MBTA's computer system, did not defraud the MBTA, and would not teach others how to do so, Sgt. Sullivan stated that they would not be subject to criminal prosecution.[27] The day after this meeting, on August 5, 2008, Anderson emailed DEFCON and stated that the meeting with law enforcement went well, and that the MIT Students' legal counsel, based on the meeting, stated that "we can definitely proceed with the talk."[28]

VI. After The August 4 Meeting, As Part Of Diligence, Senior MBTA Management Follows-Up By Asking Specifically For The Presentation Materials.

Sgt. Sullivan was concerned with the criminal aspects of the MIT Students' conduct. Senior MBTA management wanted due diligence conducted to ensure that the Students would act as they had promised, and in accordance with responsible disclosure principles.[29] Accordingly, on Wednesday, August 6, Joe Kelley contacted Professor Rivest, given his role acting on behalf of the MIT Students in setting up the first meeting. Kelley said that the MBTA wanted copies of any presentation materials, and wanted to contact the Students in further detail.

A. Through Professor Rivest, The Students Promise To Provide The MBTA With Their Presentation Materials And To Participate In A Conference Call, By Thursday, August 7.

[27] Supp. Sullivan Decl. [37] ¶¶7-8.

[28] Third Mahony Decl., Ex. 1, at MBTA22-23 ("We met with a Sargent Detective of the Intelligence unit at the MBTA and a Special Agent of the cybercrimes division of the FBI yesterday. The meeting went well, and our legal counsel has advised us that we can definitely proceed with the talk.").

[29] Supp. Kelley Decl. ¶5.

Professor Rivest said that the Students were on their way to DEFCON, but that he would get in touch with them. On August 6, that same day, Professor Rivest called back, and said that the Students would email their presentation materials to the MBTA, and would be available for a conference call the next day, Thursday August 7. [30]

B. The Students Do Not Respond, And Do Not Provide Their Presentation Materials On August 7.

When the MIT Students did not email their presentation materials, and did not make themselves available for the promised conference call, Kelley called Professor Rivest Friday August 8, 2008, at roughly 11:00 AM. Kelley again requested the presentation materials, and stated that the MBTA had to speak to the Students before the conference. Professor Rivest said he would contact the Students.

C. After Further Discussions With The MBTA, The Students Agree To Provide Presentation Materials On Friday August 8.

When the MBTA still had not received materials from the MIT Students, Scott Henderson called Anderson on the afternoon of August 8, 2008. Anderson had sent to the MBTA the Report, and Henderson had reviewed this Report. Henderson told Anderson that there was some interesting material in the Report, but that he had made many assumptions and that it was incomplete. Henderson said that it was unfortunate Anderson had not come to the MBTA to discuss his findings. Henderson then asked Anderson for a copy of the slide show presentation for the DEFCON Conference. Anderson agreed to provide this information, and this agreement is reflected in a transcribed voice-mail.[31]

D. Shortly After, On The Advice Of Their EFF Counsel, The Students Again Declined To Provide Their Slides, And Only Provided These Materials On Saturday, August 9 at 4:38 AM, The Day Of The TRO Hearing.

[30] Supp. Kelley Decl. ¶7-8.

[31] Supp. Henderson Decl. ¶¶6-8.

Shortly after finally agreeing to provide the presentation, Anderson called Henderson to say that, on the advice of counsel, he was declining to provide the materials.[32] EFF counsel admits that her clients were instructed to withhold this information from the MBTA, despite the fact that it had *already been released* to Conference attendees. EFF counsel then continued to refuse to provide the materials Friday evening and earlier Saturday morning, despite repeated requests by MBTA counsel.[33]

The MBTA still does not have complete presentation materials, despite its discovery requests.[34] As can be seen, the MIT Students declined providing the MBTA with promised materials,[35] even after, in the case of the Presentation, the undergrads knew the information was being publicly distributed.[36]

VII. The Defendant MIT Students Continue To Decline To Provide The "Key Information."

A. The MBTA Is Not Concerned With Public Domain Materials.

There are at bottom two categories of information and data that are relevant to this matter: (i) public domain materials;[37] and (ii) non-public materials that relate to the AFC system and potential security vulnerabilities. Counsel for the MIT Students, and others aligned with EFF, have referred to these non-public, AFC-related materials as the "key information" or "key

[32] Supp. Henderson Decl. ¶¶9.

[33] Supp. Mahony Decl. [9] ¶¶8-11.

[34] A Motion to Compel will follow.

[35] *See* Kelley Decl. [6] ¶¶23-26; Henderson Decl. [10] ¶13-17.

[36] *See* Mahony Supp. Decl. [9] ¶13.

[37] Public domain materials include (i) the four page Report that the MIT Students provided to the MBTA on Friday evening, August 8, the night before the initial TRO hearing was to take place (the "Report"), Compilation Ex. 20; *see* Henderson Decl. [10] ¶¶7-12, and (ii) an 87 page PowerPoint slide presentation that the MIT Students' EFF counsel refused to provide to the MBTA until 4:38 AM on Saturday morning, August 9, hours before the 11:00 AM Court hearing (the "Presentation"), Compilation Ex. 17; *see* Mahony Supp. Decl. [9] ¶¶2-13.

details." The MBTA is concerned with this "key information," and not with publicly available information.

B. "Key Information" Exists, And Has Not Been Provided.

The MIT Students seek to argue that no sensitive information remains to be disclosed, and that the protection afforded to the MBTA by the TRO is unnecessary. For example, the MIT Students argue that:

> 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.[38]

EFF counsel also argued in open court that the Presentation contained all of the information the MIT Students planned to present at the DEFCON Conference. Specifically, EFF counsel informed the Court:

> THE COURT: Just a moment. Is there anything of substance to the presentation, anticipated for the presentation that is not on the slides? MS. GRANICK: No, Your Honor.[39]
>
> ********
>
> THE COURT: All right. These are the entire materials that you intend for presentation? MS. GRANICK: Those are the visual materials. THE COURT: Well, is there anything else that is of substance for the presentation? MS. GRANICK: No, Your Honor. THE COURT: There will be nothing beyond what's shown on these several slides? MS. GRANICK: No, Your Honor…[40]

This claim is wholly inaccurate, as the Court learned over the course of the hearing. The Presentation on its face indicates the MIT Students' intent to provide additional materials,

[38] Cross Motion [26] at 5 (emphasis added).

[39] August 9, 2008 Hearing Transcript, at 7:1-7:4. (emphasis added).

[40] August 9, 2008 Hearing Transcript, at 6:12 – 6: 25 (emphasis added).

including software code, and demonstrations.[41] These additional presentation materials, of course, were identified by the MIT Students in May, when they first applied for the Conference, and specified the content of their presentation.

C. The Software Tools Are Centrally Relevant

The software tools are relevant, and have not been produced. Therefore, although EFF counsel promises the court that the tools are not malicious, there is no assurance that this is the case.[42]

D. The Demonstrations Are Also Relevant

The presentation as specified in May contained upwards of at least two demonstrations. One of those demonstrations admittedly was to show "how to create a forged card" – presumably referring to the CharlieTicket.[43]

E. The Key Information Held By The MIT Students Poses Definite Risks To The CharlieTicket System.

Since production of the Security Analysis, MBTA and vendor personnel have analyzed the document to determine the threat the information poses. Based on the evaluation of the Security Analysis document, conducted by the team reviewing the material, the MBTA has

---

[41] Compilation Ex. 17 at 105 ("For updated slides and code, see http://web.mit.edu/zacka/www/subway/"); at 142 ("wrote Python libraries for analyzing magcards"); at 171-172 (examples of code); at 191 ("Wrote code to read and clone MIFARE cards (given the key)").

[42] August 9, 2008 Hearing Transcript, at 18:9 – 18:21 ("THE COURT: All right. Now, let me focus on that issue. Ms. Granick, what's the reference to code? MS. GRANICK: The reference to code, Your Honor, relates to *the software tools that the students plan to release with the presentation and those software tools are not tools which are targeted for the MBTA system*. They are generalized, generalized tools that are for reading magnetic cards, for analyzing information on cards, and for reading, using software or open source radio software to listen to the signals from RFID cards and those sorts of things. They are not tools that a malicious attacker could come along and automatically use to crack the check sum security system, the check sum on the MBTA check sum.") (emphasis added). Interestingly, EFF counsel claimed to the Court on August 8 that the tools were going to be released. In seeking to prevent disclosure of these materials before this Court, EFF counsel now argues that the tools "were not ready."

[43] August 9, 2008 Hearing Transcript, at 9:16-9:19 ("THE COURT: So what are they going to do? MS. GRANICK: They are going to do a *demonstration* that shows that they had *now created a card that is forged*. In other words, one that is not issued by MBTA.") (emphasis added).

concluded, to a reasonable degree of certainty, the that MIT Students are able to compromise the security of the CharlieTicket system, and to clone and counterfeit CharlieTickets. Based on the Security Analysis, it appears that the MIT Students have not to date compromised the CharlieCard system.[44]

VIII. An Audit Trail Links Information In The MIT Students' Presentation With Illegal CharlieTickets, Used To Obtain Transit Services.

The MIT Students in press statements have strenuously asserted that the Students engaged in no illegal activities in conducting their purported research.[45] Indeed, EFF counsel has made similar claims, and stated to this Court that the research "was *not* obtained through any kind of unauthorized access to computers. It was research that they performed by applying existing commonly used research technique to the mag, to examine the magnetic stripe card and the data that are stored on those cards."[46] These assertions are incorrect.

MBTA personnel reviewed the MIT Students' Presentation, and particularly the images of CharlieTickets.[47] Using the AFC System's Fraud Detection features and related data, MBTA personnel linked the image of the CharlieTicket used in the Presentation to serial numbers for multiple CharlieTickets (the "Linked Tickets"). With this information, an audit trail was created, showing payments, use, other activities surrounding these Linked Tickets. This audit trail demonstrates that the Linked Tickets were used illegally, and the users of these Linked Tickets

[44] Supp. Henderson Decl. ¶¶10-13.

[45] Docket No. 31, Ex. 1 at 3 (The MBTA's complaint says that they intend to sue the students on several charges. In "Count III: Conversion," the complaint alleges that "the MIT Students exerted dominion over MBTA's property by traveling on the MBTA lines without paying fares." *But Anderson said in an e-mail that "we never rode the T for free."*) (emphasis added).

[46] August 9, 2008 Hearing Transcript, at 13:9 – 13:13 (emphasis added).

[47] Supp. Henderson Decl. ¶¶14-17.

obtained MBTA transit services without proper payment.[48] The MIT Students, therefore, have engaged in illegal activities.

Argument

I. The MBTA Is Entitled To A Preliminary Injunction

The MIT Students (i) have circumvented the security features of the MBTA's computerized CharlieTicket system; (ii) have engaged in illegal activities in the course of their conduct; (iii) have publicly offered "free subway rides for life" to interested parties over the Internet with respect to both CharlieTicket and CharlieCard passes; (iv) wish to allow others to duplicate their claimed "breaking" of the Fare Media's security systems by circulating written materials, releasing software tools, and giving demonstrations.[49]

The MBTA is entitled to a preliminary injunction because it has shown: (1) a likelihood that it will prevail on the merits; (2) irreparable harm unless the restraining order is issued; (3) greater harm to it than the adversary's harm resulting from issuance of a temporary restraining order; and (4) the absence of an adverse impact on the public interest. *Esso Standard Oil Co. (Puerto Rico) v. Monroig-Zayas*, 445 F.3d 13, 18 (1st Cir.2006); *McGuire v. Reilly*, 260 F.3d 36. 42 (1st Cir. 2001). Injunctive relief should issue to "prevent a real threat of harm." *Matos ex rel. Matos v. Clinton School District*, 367 F.3d 68, 73 (1st Cir. 2004). As demonstrated below, the MIT Students have broken the security of the MBTA's CharlieTicket, and the MBTA will suffer immediate, real harm if the MIT Students are not enjoined.

II. The MBTA Has A Substantial Likelihood Of Success On Its Claims Under The Computer Fraud And Abuse Act.

[48] Supp. Henderson Decl. ¶¶14-17.

[49] Foster Decl. ¶¶10-23; Docket No. 20, Ex. 6; Ex. 7.

The MBTA is likely to success on the merits of its claims under 18 U.S.C. §1030, the Computer Fraud and Abuse Act (the "CFAA").

A. Contrary To Their Assertions To Law Enforcement, And Their Counsel's Assertions In Open Court, The MIT Students Used CharlieTickets Illegally

The MIT Students used CharlieTickets illegally. The extent of this use remains to be quantified, as only a minor amount of usable audit information was contained in their Presentation. The MBTA believes that, with proper discovery of the Class Paper, and other materials requested to date, and more complete picture of the extent of the illegal conduct will become clear. This conduct unequivocally constitutes a violation of the CFAA.

B. The CFAA Has Been Breached By The Students' Conduct, And Without The Requested Relief Their Directed Advocacy Will Invariably Lead To Further Breaches.

Courts read a statute in accordance with its plain meaning, and unambiguous statutory language controls. *Tobib v. Radloff*, 501 U.S. 157, 162 (1991); *United States v. Ron Pair Enterprises*, 489 U.S. 235, 241 (1989). Courts, moreover, caution against reading limiting words into broad statutory language. *Tobib, 501 U.S. at 161-62* (refusing to "engraft" a requirement onto a statute's "plain language"); *Maine v. Taylor*, 477 U.S. 131, 135 (1986) (refusing to read a limitation into "the straightforward and unambiguous terms of [a] statute"); *United Union of Roofers, Waterproofers & Allied Workers v. Meese*, 823 F.2d 652, 657 (1st Cir. 1987) (Breyer, J.). The MIT Students have breached the CFAA.

First, the systems for storing value and processing payments via CharlieTickets and CharlieCards, including the Fare Gate and the Fare Vending Machine, constitute "computers" within the meaning of 18 U.S.C. §1030(e)(1). These "computers" are used in interstate commerce or communication due, for example, to the MBTA's services in Rhode Island and

Massachusetts.[50] Accordingly, these are protected computers within the meaning of 18 U.S.C. §1030(e)(2)(B).

Second, the Presentation, together with information withheld by the MIT Students to date, shows that the MIT Students have knowingly caused and, unless restrained, will knowingly cause the transmission of a program, information, code, or command targeted at MBTA protected computers. As a result of this conduct, the MIT Students intentionally caused damage without authorization, to these protected computers. Moreover, the MIT Students intentionally accessed MBTA protected computers without authorization, and as a result of such conduct, have caused damage. These damages include a loss aggregating substantially more than the $5,000 amount required under 18 U.S.C. §1030(a)(5)(B)(i), particularly in light of the volume of traffic covered by the CharlieCard and CharlieTicket passes, and the costs of the overall Automated Fare Collection System that relies on the CharlieCard and CharlieTicket passes.[51]

Finally, the damage affects a computer system used by a government entity for national security purposes, within the meaning of 18 U.S.C. §1030(a)(5)(B)(v), due to the role of the MBTA in Homeland Security efforts, and transit services generally.[52]

C. The Defendants Would Have Knowingly Transmitted Information That The Defendants Knew Would Cause Damage To Protected Computers.

The CFAA applies to the MIT Students' conduct. Judge Woodlock made detailed inquiry into each of the elements of the CFAA, and nothing has changed factually since the Saturday Hearing. For purposes of the MIT Students' challenge, only section (a)(5)(A)(i) is relevant.[53] This section reads in relevant part:

---

[50] *See* Kelley Decl. ¶7.

[51] *See* Kelley Decl. ¶¶12, 19.

[52] *See* Kelley Decl. ¶¶6, 8-9.

[53] Cross Motion [23] at 9.

> Whosoever … 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 [violates the statute][54]

The provision thus has two operative events: (i) the defendant knowingly transmits information and (ii) as a result of this conduct, the defendant intentionally – not inadvertently – causes damage to a protected computer. Here, but for the TRO, the MIT Students would have transmitted information, in the form of the Presentation and verbal presentation accompanying it, and would have transmitted code, as the Presentation also shows that MIT Students planned to provide open source software tools, to enhance attendees' hacking abilities.[55] The plain language of the Presentation demonstrates that the transmission of this information and code was knowing. Moreover, the Presentation's plain language demonstrates that the MIT Students' conduct would intentionally – and not inadvertently – cause damage to a protected computer, as evidenced by the Defendants' recognition of the illegal nature of the conduct. The conduct, therefore, falls squarely within the statute.

D. The Defendants' Construction Of The CFAA Is Illogical.

The MIT Students' construction of the CFAA leads to anomalous results. Due to time constraints, the MBTA addresses the Defendants' two primary arguments.

(1) The Statute Covers "Chains" Of Actors And Actions, And Is Not Limited To "Solo" Actors As The MIT Students' Argue.

First, the Defendants argue that a single defendant must both (i) transmit the information, and (ii) him or herself damage the protected computer.[56] The Defendants thus argue that only "solo" actors are covered by the statute. This is incorrect.

---

[54] 18 U.S.C. §1030(a)(5)(A)(i).

[55] Compilation Ex. 16 at 1, 37, 66.

[56] Cross –Motion [23] at 9 ("the offender must both transmit information to the protected computer and cause damage to that same computer.")

Certain varieties of malicious code do not become effective until an unsuspecting user opens an executable file, such as one attached to an email, that then activates the malicious code. In this situation, the individual who physically damages the computer is the unsuspecting user. Under the MIT Students' proposed interpretation, the perpetrator of the malicious code in this scenario would be free from exposure, as the perpetrator did not both "transmit" the information and damage the computer. Congress revised and updated the CFAA in part to handle more sophisticated viruses. *Violent Crime and Control and Law Enforcement Act of 1994 - Conference Report*, 103rd Cong. (1994) (Statement of Sen. Leahy). By seeking to limit the CFAA to exclude "chains" of actors and actions, the MIT Students' improperly limit the statute.

(2) The Term "Transmission" Includes Verbal Transmissions, And Cannot Be Restricted In The Manner The Defendants Claim.

Second, the MIT Students claim that the term "transmission" in section (a)(5) cannot be read to include verbal transmissions of information. This is incorrect. First, the plain meaning, dictionary definition of "transmit" is as follows:

> Transmit: 1. to send or cause to go from one person or place to another, esp. across intervening space of distance; transfer; dispatch; convey. … 4. to communicate (news, etc.) … 7. to send out (radio or television broadcasts, etc. by electromagnetic waves…. Webster's New World Dictionary (2d Ed) at 1511 (emphasis added).

The plain meaning of the term, therefore, requires the interpretation employed by Judge Woodlock.

Second, the Defendants own arguments conflict on this point. First, they assert that section (a)(1) includes a term "communicates" and the absence of this term in (a)(5) means verbal transmissions are excluded. Then the MIT Students argue that, if "transmissions" includes verbal transmissions, the CFAA would conflict with the First Amendment.[57] The

[57] Cross-Motion [23] at 11 ("the statue would be in tension with the First Amendment").

Defendants thus argue (i) that inclusion of verbal transmissions in the CFAA creates an improper conflict with the First Amendment, yet (ii) at a minimum section (a)(1) includes verbal transmissions. The argument, therefore, is inconsistent.

III. The MIT Students DEFCON Presentation First Amendment Claims Are Incorrect.

A. The Presentation Advocates Violation Of The Law And -- In The Context Of One Largest Hacker Conferences In The World -- Is Directed To, And Likely To Incite Imminent Lawless Action.

First Amendment protection does not extend to speech that advocates a violation of law, where the advocacy "is directed to inciting or producing imminent lawless action and is likely to incite or produce such action." *Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969). The MIT Students' conduct falls squarely within this well established zone of no protection. It is black-letter law that "[t]he First Amendment's guarantee of freedom of expression is sweeping, but not absolute. There are categories of speech that do not receive constitutional protection, including obscenity, defamation, fighting words, and words likely to incite imminent lawless action." *Curley v. North American Man Boy Love Ass'n,*, No. Civ.A. 00CV10956GAO, 2001 WL 1822730, *1 (D.Mass., Sep. 27, 2001) (O'Toole, J.).

Moreover, certain exercises of "speech" are "not to be protected by the First Amendment guarantee because they qualified as "incitement" to unlawful activity. Thus, speech which counsels and procures criminal conduct will support liability for "aiding and abetting" in both the criminal, *see United States v. Barnett*, 667 F.2d 835 (9th Cir.1982), and civil contexts, *see Rice v. Paladin Enterprises, Inc.*, 128 F.3d 233 (4th Cir.1997). *Curley v. North American Man Boy Love Ass'n,*, No. Civ.A. 00CV10956GAO, 2001 WL 1822730, *2 (D.Mass., Sep. 27, 2001) (O'Toole, J.).

Here, the MIT Students' conduct qualifies as "aiding and abetting." Not only are detailed instructions and demonstrations given to engage in illegal conduct, specific software tools are

provided to assist in that conduct. Because the Students have refused to provide these tools, their specifics cannot be addressed.

In addition, there is a distinction between theoretical, abstract, advocacy, and speech that constitutes specific instruction. As the *Rice* Court reasoned, "one obviously can prepare, and even steel, another to violent action not only through the dissident 'call to violence,' but also through speech, such as instruction in the methods of terror or other crime, that does not even remotely resemble advocacy, in either form or purpose." *Rice v. Paladin Enterprises, Inc.,* 128 F.3d 233, 265 (4th Cir.1997) (emphasis added). *See also United States v. Knapp,* 25 F.3d 451, 457 (7th Cir.1994); *United States v. Rowlee,* 899 F.2d 1275 (2d Cir.1990). Where a party counsels and assists others to engage in illegal acts, this conduct falls outside the zone of "mere advocacy" protected under the *Brandenburg* doctrine. *United States v. Buttorff,* 572 F.2d 619 (8th Cir.1978). Here, the MIT Students engaged in illegal activities to compile data, put that data in a "titillating" package, included specific instructions and demonstrations to show others how to copy their illegal activities, and provided specific software tools to assist. This falls well outside the zone of "mere advocacy."

This is not a case of mere "undifferentiated fear or apprehension' of illegal conduct." See *Tinker v. Des Moines Indep. Community School Dist.,* 393 U.S. at 508, 89 S.Ct. 733. Here, the DEFCON Conference is one of largest hacker conferences in the world, with an audience made up of a range of "white hats", "gray hats" and more concernedly "black hats." The fact that the MIT Students have, in fact, compromised the CharlieTicket system – and audit trails show their specific illegal conduct -- demonstrates this specific illegal conduct at issue.

The Presentation, and likely the related code and materials, unequivocally constitute advocacy in favor of a violation of law. The Presentation, standing alone, shows this. For example, the MIT Students (i) expressly promise "you now have free subway rides for life";[58] (ii) admit "THIS IS VERY ILLEGAL"[59]; and (iii) recognize the risks of court involvement, stating for example, "what this talk is not: evidence in court (hopefully)."[60]

Moreover, in the Presentation, the MIT Students promise attendees that:

> "You'll learn how to generate stored-value fare cards; reverse engineer magstripes; hack RFID cards; use software radio to sniff; use FPGAs to brute force; tap into the fare vending network; social engineer; WARCART![61]

And they further instruct attendees "to execute these attacks we need to interact with the card."[62] As a final example, the MIT Students provide a photo of an MBTA network switch, which can only be accessed via a trespass onto MBTA property, and then they visually associate the network switch with "Wireshark," a software application that sniffs and captures data from a network: further illegal activity. In sum, the MIT Students are vigorously and energetically advocating illegal activity, and this advocacy, in the context of the DEFCON Conference, is both directed to inciting or producing imminent lawless action, and likely to produce such action. In sum, speech used to further an illegal activity is not constitutionally protected." *U.S. v. Kaun*, 827 F.2d 1144, 1152 (7th Cir. 1987). That is the speech at issue here.[63] Therefore, the MIT Students enjoy no protections under the First Amendment.

---

[58] *See* Compilation Ex. at 129 (emphasis added).

[59] *See* Compilation Ex. 16 at 109 (emphasis added; capitalizations in original) (the "Presentation").

[60] Compilation Ex. 16 at 107 (emphasis added).

[61] Compilation Ex. 16 at 4.

[62] Compilation Ex. 16 at 47.

[63] The MBTA relies on its Opposition to Cross-Motion for Reconsideration for its arguments as to commercial speech.

IV. The MBTA Will Suffer Irreparable Harm Without The Requested Relief.

"Irreparable injury' in the preliminary injunction context means an injury that cannot adequately be compensated for either by a later-issued permanent injunction, after a full adjudication on the merits, or by a later-issued damages remedy." *Rio Grande Cmty. Health Ctr., Inc. v. Rullan*, 397 F.3d 56, 76 (1st Cir. 2005). The loss of a trade secret is generally found to constitute irreparable harm. *TouchPoint Solutions, Inc. v. Eastman Kodak Co.*, 345 F.Supp.2d 23, 32 (D.Mass. 2004). That is in recognition of the fact that, "once the trade secret is lost, it is gone forever." *Id. (citing FMC Corp. v. Taiwan Tainan Giant Indus. Co.,* 730 F.2d 61, 63 (2d Cir.1984)).

Here, the MBTA has determined, based on the Security Analysis that the MIT Students have compromised the CharlieTicket, and are able to clone and counterfeit CharlieTickets. Moreover, based on the audit trail analysis, the MBTA has located these types of illegal CharlieTickets, and have linked them to information in the Students' Presentation. Therefore, the Students have the ability to cause significant harm to the CharlieTicket system, during the roughly five-month window that remedial actions will require. The requested relief, therefore, is necessary to preserve the status quo until this remedial activity is complete. *See CMM Cable Rep., Inc. v. Ocean Coast Properties, Inc.*, 48 F.3d 618, 620 (1st Cir.1995).

A. The MBTA Seeks Injunctive Relief Of Limited Duration, Extending Only Five Months To Allow Completion of Remedial Measures.

The MBTA and its vendors have evaluated the Security Analysis, and have concluded that the MIT Students have compromised the security of the CharlieTicket. With its vendors, the MBTA has concluded that planning and implementing remedial measures will require approximately five months.[64] The MBTA limits its request for injunctive relief accordingly.

[64] Supp. Henderson Decl. ¶18.

V. The Balance Of Harms Lies Decisively In The MBTA's Favor.

The MBTA will unequivocally suffer the greater harm, if the requested relief is not continued.

A. The MIT Students Knew Of The MBTA's Requests For Their Presentation Materials Well Before The Presentation; Indeed The Students Still Decline To Produce Presentation Materials, Such As Their Software Tools.

The MIT Students knew or by law are deemed to have know of the MBTA's requests for their presentation materials after the August 4 meeting. Professor Rivest, through whom the MIT Students dealt, was their agent, and his knowledge of the requests, at a minimum, is attributed to the Students. Professor Rivest at a minimum held apparent authority on behalf of the MIT Students. Apparent authority "results from conduct by the principal which causes a third person reasonably to believe that a particular person has authority to enter into negotiations." *Linkage Corp. v. Trustees of Boston, Univ.*, 425 Mass. 1, 31 (1997); *see also* Restatement (Second) of Agency, § 8; *Theos & Sons, Inc. v. Mack Trucks, Inc.*, 431 Mass. 736, 745 (2000) ("Apparent authority is created to a third person by written or spoke words or any other conduct of the principal which, reasonably interpreted, causes the third person to believe that the principal consents to have the act done on his behalf by the person purporting to act for him.").

Here, in statements to the press, the Students admit that they dealt through Professor Rivest.[65] Sgt. Sullivan, in setting up the August 4 meeting, worked through Professor Rivest, and the MIT Students attended the meeting. Moreover, the MIT Students originally obtained a two week period to provide the "vulnerability report" to the MBTA. After the MBTA's

[65] Docket No. 31, Ex. 1 at 3 ("The students had also been in contact with the MBTA since July 31 *through Ronald L. Rivest*, the professor who had overseen their 6.857 project") (emphasis added).

discussions with Professor Rivest, the Students shortened this deadline to Friday, August 8: demonstrating discussions between Rivest and the MIT Students.

Moreover, even if the Students did not know of the requests for the materials until Friday, and even if Professor Rivest were not acting as their agent for this purpose, when the Students and their EFF counsel unequivocally knew of the request for presentation materials, they still declined to provide this information until Saturday, early morning.

B. The MIT Students Have Engaged In Illegal Conduct, Yet Have Not Provided The Level Of Disclosure And Assistance To The MBTA That Might Excuse Their Illegal Means For A "Better Security" End.

The MIT Students have engaged in illegal conduct, and have used their techniques to improperly to obtain transit services at no cost. Even if one were to excuse this illegal behavior as a necessary means to uncover security flaws, the MIT Students have refused to undertake the "quid pro quo" of full disclosure and assistance to remedy the flaws identified. Accordingly, if the goal of the MIT Students' view of responsible disclosure is "better security for all", their strategy seems poorly designed for this end. This strategy deserves no weight in balancing the parties' conflicting harms.

A. The TRO Does Not Prevent The Defendants From Engaging In Any Of The Activities They Identify.

The MIT Students' own arguments demonstrate that the TRO does not prevent them from undertaking any activities they had intended. EFF counsel asserts that:[66]

> [T]he students have repeatedly told the MBTA that the students never intended to disclose key details in the public presentation.[67]

[66] As with all statements concerning the MIT Students, no MIT Undergrad testimony is presented in support.

[67] Cross Motion [23] at 6 (emphasis added).

Further, EFF counsel states, in arguing that the MIT Students have, and will comply with the EFF's formulation of "Responsible Disclosure":

> Withholding key information about the flaws one discovers while publishing other information, as the students here did, is responsible.[68]

Nothing in the original TRO, or in the TRO with proposed modifications by the MBTA, would prohibit the MIT Students from publishing or speaking about their project, provided they withheld this "key information" and "key details." In sum, the TRO language does not prohibit the MIT Students from engaging in any conduct they originally planned.

B. Under Industry-Recognized "Responsible Disclosure" Practices, There Will Be No Cognizable Harm To The MIT Students.

The temporary halt on the MIT Undergrad's disclosures will not create cognizable harm to the defendants. This is particularly true in light of industry practices, and the so-called "responsible disclosure" doctrine. The plaintiff briefed these principles in its Memorandum in Support of Motion for Temporary Restraining Order,[69] and incorporates these points by reference.

The MIT Students seek to rely on a proposed definition of "Responsible Disclosure" that is illogical[70] and inapplicable.[71] As demonstrated above, the Professors' letter -- on which the MIT Students base their claims – is based on incorrect factual assumptions. Accordingly, it is inapplicable.

VI. The Requested Relief Furthers The Public Interest.

---

[68] Cross Motion [23] at 5 (emphasis added).

[69] *See* Memorandum in Support of Motion for TRO [3] at iv-vi.

[70] This argument is made in the MBTA's Opposition to the Cross-Motion to Reconsider [30] at 13.

[71] The Professors and others who assented to the "Letter From Computer Science Professors and Computer Scientists" attached as Exhibit A to the Declaration of Marcia Hofmann, fall to the same illogic.

The final factor is the public interest. This factor requires the Court to "inquire whether there are public interests beyond the private interests of the litigants that would be affected by the issuance or denial of injunctive relief." *Friends of Magurrewock, Inc. v. U.S. Army Corps of Engineers*, 498 F.Supp.2d 365, 379 (D.Me.,2007) (quoting *Everett J. Prescott, Inc. v. Ross*, 383 F.Supp.2d 180, 193 (D.Me.2005))

The MBTA provides approximately 1.4 million passenger trips per weekday.[72] The Fare Media System threatened by the MIT Students' conduct governs the majority of this system. It is strongly in the public interest to protect this system in the manner requested, particularly in light of the steps the MBTA has taken to avoid the necessity of requesting further relief from this Court, and the time-limited nature of the request Preliminary Injunction.

The MBTA's primary goal in this matter is to understand the threat to its Fare Media System, including related illegal activity by the MIT Students, so that it can remedy this threat and take steps to avoid a similar threat in the future.

Under no interpretation of the term have the MIT Students engaged in "Responsible Disclosure" here. For sure, the public has a strong interest in resolving security flaws, and in avoiding "puffing" and false claims of "security" by entities that rely on network and computing security. Yet that is not the situation here.

The MBTA does not seek to stop the MIT Students or any others from discussing the state of the MBTA's security. The MBTA seeks only to prevent premature disclosure of "key information" concerning potential and actual vulnerabilities of its Fare Media System. There is no public interest in college students' publicly claiming abilities to "defraud public agencies," undertaking illegal activities to accomplish this result, teaching others with specific software and

[72] Kelley Decl. ¶6.

other tools to copycat this result, and then refusing to discuss the details of their "accomplishments" to allow the public entity to take necessary steps to mitigate the risk.

Conclusion

THEREFORE, the plaintiff respectfully requests that this Court enter the attached proposed Order.

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY

By its attorneys,

/s/ Ieuan G. Mahony
Ieuan G. Mahony (BBO #552349)
Maximillian J. Bodoin (BBO # 667240)
HOLLAND & KNIGHT LLP
10 St. James Avenue
Boston, MA 02116
(617) 523-2700

Thomas F.S. Darling III (BBO #558848)
MASSACHUSETTS BAY TRANSPORTATION AUTHORITY
State Transportation Building
7th Floor
10 Park Plaza
Boston, MA 02116
(617) 222-3174

Dated: August 18, 2008
Boston, Massachusetts

CERTIFICATE OF SERVICE

I, Ieuan G. Mahony, Attorney for the Massachusetts Bay Transportation Authority in connection with the above-captioned proceeding, hereby certify that on this 18th day of August, 2008, the Memorandum in Support of Plaintiff's Motion to Convert Temporary Restraining Order to Time-Limited Preliminary Injunction--Leave to File Granted on August 18, 2008 was served via the ECF system on the following interested parties:

Party	**Counsel**
Zack Anderson, RJ Ryan, and Alessandro Chiesa (the "MIT Undergrads")	Emily Berger, Esquire Email: emily@eff.org Jennifer Granick, Esquire Email: jennifer@eff.org John Reinstein, Esquire Email: reinstein@aclum.org Thomas A. Brown Email: tbrown@fr.com Cindy Cohn cindy@eff.org Lawrence K. Kolodney kolodney@fr.com Marcia Hoffman marcia@eff.org Adam J. Kessel kessel@fr.com
Massachusetts Institute of Technology ("MIT")	Jeffrey Swope, Esquire Email: JSwope@eapdlaw.com

/s/ Ieuan G. Mahony