UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MASSACHUSETTS BAY TRANSPORTATION AUTHORITY Plaintiff v. ZACK ANDERSON, RJ RYAN, ALESSANDRO CHIESA, RONALD L. RIVEST, and the MASSACHUSETTS INSTITUTE OF TECHNOLOGY Defendants	Civil Action No. 08-11364-GAO

DECLARATION OF MAXIMILLIAN J. BODOIN IN SUPPORT OF MOTION FOR ENTRY OF PRELIMINARY INJUNCTION

1. I am an associate at Holland & Knight, LLP, representing Plaintiff, Massachusetts Bay Transportation Authority ("MBTA") in this matter. This Declaration is submitted in support of the MBTA's Motion for Entry of Preliminary Injunction and Memorandum in Support of its Motion for Entry of Preliminary Injunction. I make this Declaration based on a search of publicly available information on the Internet.

2. Attached as Exhibit 1 is a true and accurate copy of an abstract of a paper by Arias Hung entitled "*Owning the Linksys wrtp54g VOIP Router.*" *See* http://www.defcon.org/html/defcon-14/dc-14-speakers.html. According to the summary, Mr. Hung's presentation included "a demonstration of how easy VOIP and its companion protocol MGCP can be manipulated for illegal purposes such as call spoofing, number hijacking, and untraceable call routing." *See* Exh. 1.

3. Attached as Exhibit 2 is a true and accurate copy of an article dated August 7, 2007 and entitled "*Middle America, Meet the Hackers.*" *See*

http://www.forbes.com/2007/08/06/security-hacking-challenge-tech-cx_ag_0806toughhack.html. The article states that DEFCON " … still attracts some true 'black hat' hackers, bent on learning the newest tools for illegal intrusion, sabotage, espionage and credit card theft." *See* Exh. 2. The article also quotes a DEFCON organizer: "When DefCon's hackers do venture into the illegal, it's often based on impulses that are more libertarian than malicious, says a hacker known as 'Dead Addict,' another of DefCon's organizers. 'We simply don't take the law as a moral compass,' he says." *See id.* at p. 2.

4. Attached as Exhibit 3 is a true and accurate copy of a post on August 9, 2008 and entitled "*Shrinky Dinks as a Threat to National Security*." *See* http://it.slashdot.org/article.pl?sid=08/08/10/0013226&from=rss. This post states that, at the DEFCON Convention, Marc Weber Tobias demonstrated a method of picking the "'high-security' locks that protect the White House, the Pentagon, embassies, and many other sensitive locations." *See* Exh. 3. The post states that, using the demonstrated method, one was "… able to open an example lock in about six seconds." *Id.*

5. Attached as Exhibit 4 is a true and accurate copy of an article by Robert Lemos entitled "*Russian Crypto Expert Arrested at Def Con*" dated July 17, 2001. *See* http://news.cnet.com/2100-1001-270082.html. The article states that a DEFCON speaker, Dmitry Sklyarov, was arrested a day after his presentation at the DEFCON Convention. *See* Exh. 4. The article states that the Federal Bureau of Investigation "… acknowledged Tuesday that it had arrested security researcher Dmitry Sklyarov for what it said was a violation of the Digital Millennium Copyright Act." *Id.*

6. Attached as Exhibit 5 is a true and accurate copy of an article by Erik Larkin entitled "*Simple Hack Can unlock Most Any Office Door*" dated August 4, 2007. *See*

http://blogs.pcworld.com/staffblog/archives/005079.html. The article discusses a DEFCON demonstration by a hacker and DEFCON staffer identified as Zac Franken. *See* Exh. 5. According to the article, Mr. Franken's demonstration provided instructions for hacking into card readers often found on office doors by using a home-made device comprising of approximately $10 worth of components, called the "Gecko." *See id.* The hack was used to "subvert[] the Wiegand protocol, commonly used for communication between the card reader and the back-end access control system..." *Id.* The demonstration also provided information on how an invader could lock authorized users out of the security system – "[w]ith nobody else able to use that door, an invader would have plenty of time to steal data or work his mischief." *Id.* The demonstration also contained instructions for how and where to splice into wires attached to the security card readers. *Id.*

Signed under the penalties of perjury this 18th day of August, 2008.

Maximillian J. Bodoin

5548457_v2

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 **Declaration of Maximillian J. Bodoin in Support of Motion for Entry of Preliminary Injunction** 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