UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	**Criminal No. 11-10260-NMG**
	)	
AARON SWARTZ,	)	
Defendant	)	

MOTION OF THE UNITED STATES FOR A PROTECTIVE ORDER

The United States moves the Court to enter the attached protective order. The order is necessary to protect victims in the case from the very real risk of serious and irremediable harm while permitting the effective production of additional materials pursuant to Fed. R. Crim. P. 16 and the Local Rules of this Court.

As the Court is aware, Aaron Swartz is charged with illegally accessing MIT's computer network and, through it, stealing a major portion of JSTOR's valuable digital database. While some peripheral facts will likely be disputed at trial, much of the evidence that cannot be disputed (university records, computer logs, records from one of Swartz's own computers, and surveillance camera recordings) demonstrate that Swartz:

1. was not a student, faculty member or employee of MIT;

2. gained physical access to MIT's computer network through a laptop computer he had installed in a restricted wiring closet in the basement of a research building;

3. intentionally masked his face with a bicycle helmet to avoid identification on a video camera as he entered the closet to remove the laptop;

4. used fictitious names and manipulated computer identification information to get and maintain access to MIT's computer network;

5. took repeated and affirmative steps to evade efforts by both MIT and JSTOR to lock him out of their computer networks;

6. downloaded a major portion of JSTOR's valuable digital database of scientific journals over the course of three months; and

7. earlier posted on one of his websites, guerrillaopenaccess.com, a call-to-arms entitled "Guerrilla Open Access *Manifesto*" which concluded "We need to download scientific journals and upload them to file sharing networks. We need to fight for *Guerrilla Open Access*." (Emphasis in the original.)

In this context, Aaron Swartz cannot be entrusted with responsibly protecting confidential internal records of MIT and JSTOR. These include databases, private electronic communications and records that are either very valuable or that could cause great damage if released to the public:

1. several million JSTOR articles that Swartz downloaded;

2. a software program Swartz used during his automated theft from JSTOR (and a variant of it);

3. discussion and analyses of Swartz's illegal access to MIT's network and possible means to defend against it;

4. analyses of methods used by Swartz during his automated theft from JSTOR and internal discussions on possible ways to stop it; and

5. descriptions of the networks' and databases' vulnerabilities.

The United States does not seek to withhold discovery of these items from Defendant or his defense counsel. Quite the contrary. The United States wants to produce this material, in many cases well ahead of the deadlines set by statute and the Local Rules. The proposed protective order, however, is critically necessary to prevent irreparably harmful redistribution of the material, whether intentional or unintentional.

The government's protective order proposes two levels of protection. The greatest is accorded the extensive database of digitized scientific articles that Defendant downloaded with his automated attack. These articles are JSTOR's lifeblood. JSTOR has spent millions of dollars to locate articles, work out copyright deals, digitize the articles, store them, and make them available online.[1] Accordingly, these articles should be protected by being maintained at government offices. The government can secure this data to an extent that a law office cannot. If and when the defense wishes to examine it, the government will make a copy available for examination with the assistance of an agent otherwise uninvolved in the case, who will be instructed not to communicate with the prosecution team about what items the defense reviews except at the request of the defendant or with prior approval of the Court. (The government does not expect the defense counsel, experts, or investigators to mishandle the evidence, whether at the government's offices or at their own. Rather, the government proposes to keep the articles in the government's custody because they will be safest there, including from unrelated third parties who might wish to access them.)

An important but less restrictive protection is accorded to the rest of the discovery materials, including the confidential records of victims MIT and JSTOR, Swartz's programs for downloading articles, and analyses of downloading methods or network vulnerabilities. Copies of these would be provided to defense counsel, but their custody would be limited to his office and the office of whichever experts and investigators that Defendant might retain. Defendant himself could review these materials at their offices and under their supervision.

---

[1] A JSTOR representative will address this issue before the Court at the hearing on this motion.

The government's protective order would not unfairly impede Defendant's ability to assist in the preparation of his defense. The United States does not seek to limit these discovery materials to his attorneys' eyes only. Rather, Defendant could review the materials at a variety of locations: the offices of his defense counsel, his expert witnesses, or his private investigators. Just as the United States did not oppose Defendant's bid to move outside the District, the United States does not seek to limit the geographic location of his attorneys, experts, or investigators that he hires, nor their number. But limiting his contact and review of these records to those custodians' offices is necessary. In a case that involves sensitive information, Defendant can be expected to go through reasonable security measures to access that information.

The United States' proposal is reasonable: you don't put a multimillion dollar database and discussions of its vulnerabilities in the custody of the person accused of stealing it.

If the Court seeks to compromise by asking the United States to cull through the discovery materials and designate page by page which documents would be stored with defense counsel and which with Defendant, the United States will comply.[2] But doing so would seriously delay production. There are a lot of pages to go through page-by-page. Rather, the United States would prefer to disclose its discovery early. The government's protective order would allow this early discovery.

For these reasons, the United States moves the Court to enter the attached protective order.

---

[2]The protective order already specifies an easily definable subset of documents that Defendant could store at his residence: fingerprint analyses, photo spreads, search warrants and supporting affidavits.

Respectfully submitted,

Carmen M. Ortiz
United States Attorney

By: */s/ Scott L. Garland*
Stephen P. Heymann
Scott L. Garland
Assistant U.S. Attorneys

CERTIFICATE OF SERVICE

I hereby certify that these documents are being filed through the ECF system and therefore will be sent electronically to the registered participants as identified on the Notice of Electronic Filing.

/s/ Scott L. Garland
Scott L. Garland
Assistant U.S. Attorney

Date: September 27, 2011