Exhibit 1

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

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

(PROPOSED) ORDER

After consideration of the Government's motion for a protective order, the Defendant's motion to compel discovery, and the oppositions filed by both parties in response to the motions, it is ordered that the Government shall provide copies, or enable the Defendant to make copies, of the following that are within its possession, custody or control:

1. All electronic data that constitutes or includes a written statement of Mr. Swartz including communications on Twitter, Facebook, text message and email or any other form of electronic communication.
2. All data, documents, and tangible things including, but not limited to, data obtained from MIT and JSTOR, that are discoverable under Rule 16(a)(1)(E). All data includes: (A) all data seized from devices that the government has asserted belong to the defendant, including:

    - Acer laptop computer recovered at MIT
    - Four Samsung hard drives delivered to the Secret Service by Defendant Swartz and his counsel on June 7, 2011
    - Western Digital hard drive recovered at MIT*
    - HP USB drive seized from the defendant at the time of his arrest
    - Apple iMac computer seized at Harvard

* Search warrant applications for devices seized at MIT and Harvard allege probable cause to believe that these devices belong to Mr. Swartz and are evidence of the commission of the offenses charged in the indictment.

- Western Digital hard drive seized at Harvard
- HTC G2 cell phone seized during the search of the defendant's residence
- Nokia 2320 cell phone seized during the search of the defendant's residence
- Sony Micro Vault seized during the search of the defendant's residence

(B) All data and items that are material to preparing the defense, namely, all data and items that constitute, or are evidence of, the occurrences and activity, including electronic communications, transmissions, and activity, that the government alleges occurred in the indictment.

(C) All data and items that the government intends to use in its case-in-chief.

(D) With respect in particular to any and all data that the government alleges was illegally downloaded from JSTOR's database including, but not limited to the data stored in the Four Samsung hard drives delivered to the Secret Service by Defendant Swartz and his counsel on June 7, 2011 ("the downloaded data"), the government shall provide one bit by bit copy of the downloaded data in its native format to the defense at the office of Collora LLP, 400 Atlantic Avenue, Boston, into the custody of Attorney William Kettlewell who shall sign a copy of this order. Access to the room in which the downloaded data shall be stored at Collora LLP shall be controlled by keys to be kept in the sole custody of Mr. Kettlewell and Andrew Good. The downloaded data in the custody of Mr. Kettlewell and Mr. Good shall be accessed solely on an offline computer that is not connected to the internet. Until and unless this Court approves a written modification of this order, each member of the defense, including Mr. Swartz, may have access to the

downloaded data in the offices of Collora LLP, and at no other location, and only after signing a copy of this order.

(E) In the event that the defense electronically transmits copies of any or all of the nine email chains designated by the government by means of any form of internet communication including email, access to copies of any of the nine email chains must be protected by a privileged password.

3. All data, documents, and tangible things that constitute or are evidence of the potentially exculpatory information described in paragraph H.1 and H.5 of the government's August 12, 2011 letter to defense counsel other than the fingerprint data that has already been produced.
4. Full and complete copies of all video recordings made inside the closet in the basement of MIT Building 16 including, but not limited to, recordings made on January 4 and 6, 2011.
5. All data, documents, and tangible things that constitute or are evidence of the eyewitness identification procedure mentioned in paragraph G of the government's August 12, 2011 letter to defense counsel.

When the data referred to in this order is computerized electronic data, transmissions, or communications, the government shall provide copies, or enable the defense to make copies, of the data in its native, bit-by-bit form, including all metadata, if the government has the data in its native format including all metadata. If the government does not have the data in its native form, including all metadata, it is to provide copies or enable the defense to make copies in the same computer searchable format of the data that is within in the possession, custody and control of the government, including optical

character recognition software format.

Any and all documents and information provided to Mr. Swartz, his counsel, his counsel's investigators and defense are to be used solely for the litigation of this case and no part of the documents or information may be disclosed or used for any other purpose.

SO ORDERED.

_____

JUDITH G. DEIN
United States Chief Magistrate Judge

Date: