UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

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

DEFENDANT AARON SWARTZ'S SUPPLEMENTAL SUBMISSION IN SUPPORT OF HIS MOTION TO COMPEL DISCOVERY AND A PROTECTIVE ORDER

Aaron Swartz provides this supplemental submission to address certain issues raised during the October 11, 2011 hearing. The Court identified two categories of discoverable data:

(1) the data allegedly downloaded from JSTOR's website; and

(2) nine email chains of communications between MIT and JSTOR about the downloading and vulnerabilities that allegedly enabled or might enable downloading to occur.

I. THE DOWNLOADED DATA.

A. Security Arrangements.

Both in its motion seeking a protective order and at the hearing, the government attempts to justify an order that the defense be required to use the downloaded data to litigate this case and prepare for trial solely in a Secret Service office. Its insistence on keeping the data solely in the government's possession is based on a claim that "The government can secure this data to an extent that a law office cannot." Motion of the United States for a Protective Order, Dkt 18, at 3. The government claims that it is primarily concerned with preventing third parties from obtaining access to the

downloaded data. *Id*. It agrees that the defense counsel and its experts and investigators can be trusted to use the data lawfully. It has presented no evidence that Mr. Swartz cannot be similarly trusted to use the information exclusively for the defense of this case. Neither the government nor the Court can deny that Mr. Swartz is the most important member of the defense team who must examine and analyze discoverable data, including the downloaded data.

The government cannot and does not deny that the defense's searches and other work with the downloaded data is privileged information. The defense's selection of searches and other examinations of the downloaded data would be recorded in electronic data that would remain in the government's possession. For that reason, if its proposed protective order is approved by the Court, the government would have impermissible and unconstitutional access to the defense's work product-protected data. *See United States v. Horn*, 29 F.3d 754, 757-758 (1st Cir. 1994)(government surveillance of defense's selections from discoverable documents constitutes prosecutorial conduct).

The defense proposes that the downloaded data be provided to it at the offices of Collora LLP, which is on the 12th floor of the Federal Reserve Bank Building in Boston. That building and office is at least as secure as any other government building and office in Boston, including the US Attorney's office and the Secret Service office. The downloaded data would be stored in a locked space within the Collora LLP office suite. The keys would be possessed exclusively by undersigned counsel and William Kettlewell, a Collora LLP partner who was a consultant on the defense team prior to the indictment who met with the government and undersigned counsel prior to the indictment, and remains a member of the defense team without having filed his

appearance. Mr. Kettlewell is willing to sign a protective order, as are the defendant and all members of the defense team. The data would be stored and accessible only on an off-line computer at Collora LLP that is not connected to the Internet. In the event that the defense contends that it is necessary to modify the restrictions on storage, access and use of the downloaded data, the defense would be required to seek court approval. Terms for such a protective order are attached hereto as Exhibit 1.

B. Severance of Metadata From Articles and Other Text.

At the hearing, the Court ordered the government to inform the Court whether it is feasible to sever the metadata from the articles to which the metadata relates. The government has informed the defense counsel that it proposes to provide the defense with the metadata without the pdf files to which the metadata relates. The defense is entitled to, and must have, the same full set of downloaded data, including the pdf files that the government has, in order to litigate this case through a trial. Without the articles and other pdf files, the defense cannot effectively and efficiently conduct its analysis of exactly what was downloaded from where and under what circumstances. The metadata alone does not provide this essential set of full information. In view of the security arrangements proposed by the defense, there is no justification for redacting discoverable data and subjecting the defense to an unconstitutional burden of having to seek essential information about the downloaded data from the government. These defense requests would, in turn, disclose work product privileged information. The defense cannot be required to conduct this litigation without information that Rule 16 entitles it to have in order to provide even-handed access to evidence and information.

II. THE NON-DOWNLOADED DATA.

The government proposes that Mr. Swartz be prohibited from receiving copies of nine email chains. Instead, it proposes that Mr. Swartz read, and work at his counsel's office with, these nine email chains pertaining to "security weaknesses" of MIT's and JSTOR's computer networks. Mr. Swartz is willing to sign a protective order restricting his use of this information to the litigation of this case. That is all that is necessary to provide a more than sufficient assurance against any improper or unlawful use of copies of these email chains.

The defense team, including Mr. Swartz, his lawyers, investigators and experts, are located in several cities, only one of which is Boston. Communication of privileged information within the defense camp occurs by password-protected, confidential email. Arguendo, even if the government's mistrust of Mr. Swartz is taken at face value, its proposal does not afford any substantial security against improper use of this discoverable information. Mr. Swartz must and will have all of the information in these nine email chains. These emails about means of access to MIT and JSTOR networks, characterized by the government as "vulnerabilities," may contain important exculpatory information, or may lead to exculpatory evidence. There is no basis in this record for Mr. Swartz to be the only member of the defense team who can have this information, but cannot have copies, to use for his defense.

Mr. Swartz must be able to make notes and send memoranda to the defense team about these nine emails after studying them up to and including the trial. He is not usually in Boston during the work week. He must work on this case on nights and

weekends. As to these nine email chains, the defense would transmit them as password-protected documents sent by electronic mail. The defense is willing to password protect these particular discovery materials by circulating them electronically among members of the defense team as provided in Exhibit1.

In any event, based on this record, this Court should view with skepticism the government's unsupported claim that disclosure of the nine email chains threatens harm to either MIT or JSTOR. There is no affidavit or evidence in any form to support that claim. JSTOR's counsel did not express concern about any non-downloaded data including its communications with MIT or anyone else. MIT has not objected to disclosure of this supposedly sensitive information either. Even if MIT or JSTOR objected to disclosure, these documents are putative evidence that the defense may be entitled to admit during Mr. Swartz's public trial. Because these documents are potential evidence in a public trial, refusing to make copies available to Mr. Swartz cannot be justified. The government has abandoned its claim that Mr. Swartz cannot be trusted to have a copy of three lines of code he allegedly wrote and used to download data. It has unjustifiably withheld huge amounts of discoverable data for weeks by making wildly unsupported security claims that it has now abandoned. Mr. Swartz should have copies of the nine email chains exclusively for his use in defending this case.

III. THE SEIZED DATA, DEFENDANT'S STATEMENTS, AND EXCULPATORY EVIDENCE

The Court should order the government to provide copies of the following:

1. **Defendant's Written Statements.** The defendant's written statements that are within its custody, possession and control, e.g., Twitter and Facebook postings,

websites, text messages and electronic mail. The government obtained some of this information as the fruit of warrantless seizures of devices that the government asserts belong to Mr. Swartz; some are the fruit of warrant-authorized seizures of items that the government asserts belong to Mr. Swartz; and some information was obtained in response to grand jury subpoenas to electronic communications providers. The defendant's written statements are subject to automatic discovery. Local Rule 116.1(C)(1)(a) and Rule 16(a)(E). In paragraph A.1.a. of its August 12, 2011 letter to defense counsel (attached hereto as Exhibit 2), the government states that it will offer some of these written statements in its case-in-chief. The defendant's written statements are also material to the defense. The government does not provide any "good cause" for withholding the defendant's written statements.

2. **Seized Electronic Data.** In its August 12, 2001 letter, the government listed the items containing electronic data stored in electronic data storage media that it has seized as follows:

- Acer laptop computer recovered at MIT
- 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
- 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

The government has no good cause to withhold copies of the seized electronic data, all of which is discoverable under Rule 16(a)(1)(E). For that reason, the

* 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.

instant motion seeks an order compelling the government to provide the defense with copies in the form of bit-by-bit, mirror electronic images of all of the data natively stored on the above-listed electronic devices, including any and all metadata. In order to effectively defend himself against the indictment's allegations, Mr. Swartz is constitutionally entitled to an exact and complete copy of the discoverable electronically stored information in its native format so that he may examine and, if appropriate, contest the provenance and substance of that evidence. *See United States v. Briggs, 2011 U.S. Dist. LEXIS 101415 (W.D.N.Y.).*

3. **Complete Video Recordings.** Paragraph E of the government's August 12, 2011 letter states that it has provided copies of what it considers to be the "relevant portions" of video recordings made on January 4 and 6, 2011, in a wiring closet in the basement of MIT's Building 16. Under Rule 16, Mr. Swartz is entitled to full and complete copies of all video recordings made in that closet including but not limited to recordings made at any time including, but not limited to, January 4 and 6, 2011, because the complete records contain evidence that is material to his defense.

4. **Exculpatory Evidence**. In paragraph H of the government's letter, the government described but refused to provide almost all of certain exculpatory evidence, including evidence that, during the period covered by the indictment, persons other than Mr. Swartz at Harvard, MIT and China accessed the Acer laptop that was seized by the government, and persons other than Mr. Swartz at MIT and elsewhere were engaging in "journal spidering" of JSTOR data using a "virtual computer" that can be hosted by anyone at MIT. The government has no

basis for withholding the electronic evidence described as exculpatory in its letter.

CONCLUSION.

For all the foregoing reasons, the Court should enter the order attached hereto as Exhibit 1.

Respectfully submitted,

/s/Andrew Good
Andrew Good
BBO # 201240
Good & Cormier
83 Atlantic Avenue
Boston, MA 02110
Tel. 617-523-5933
agood@goodcormier.com

CERTIFICATE OF SERVICE

I hereby certify that the foregoing document filed through the ECF system will be sent to counsel for the government who are registered participants as identified on the Notice of Electronic Filing ("NEF").

DATED: October 24, 2011

/s/ *Andrew Good*
Andrew Good

G:\CLIENTS\Swartz, Aaron\Pleadings - Federal Court Case\Supplemental Submission in Support of Motion to Compel.doc