UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

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

DEFENDANT'S MEMORANDUM OF LAW
IN SUPPORT OF HIS MOTION TO COMPEL DISCOVERY

Pursuant to Local Rule 116.3(G) and the September 9, 2011 order of this Court, Aaron Swartz moves this Court for an order compelling the government to provide discovery as provided by F.R. Crim. Proc. 16 and by the automatic discovery provisions in Rules 116.1(A)(1) and (C) and 116.2. The government has not provided a very substantial portion of the information and documents required to be disclosed by these rules. Instead, it has withheld automatically discoverable information and documents, and demanded that the defense agree to an unjustified protective order as a pre-condition to receipt of discovery. Without good cause, the government has withheld 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 1), 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 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 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

* 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.

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. **Electronic Data Obtained From Non-Parties.** The government's August 12, 2011 letter states all documents and tangible objects that are material to the defense including, but not limited to, items obtained from MIT and JSTOR are being withheld. In its letter, the government asserts that:

> Because many of these items contain **potentially** sensitive, confidential, and proprietary communications, documents and records obtained from MIT and JSTOR, including discussions of victims' computer systems and security measures, we will need to arrange a protective order with you before inspection.

Exhibit 1 at 2 (emphasis added). Rule 16(d)(1) authorizes this Court to enter protective orders concerning information provided in discovery. However, the movant for such a protective order must make a showing of "good cause" for the entry of such an order.

The First Circuit has not provided guidance to the lower courts concerning the factors to be taken into account in determining whether a movant has shown Rule 16(d)(1) "good cause," except in cases involving disclosure of classified national security secrets under the Classified Information Procedure Act (CIPA). *United States v. Pringle*, 751 F.2d 419, 427-428 (1st Cir. 1984). Certainly, the information being withheld is not classified as secret for national security reasons. There is no allegation that the withheld information concerns an endangered confidential informant, or that there is any evidence to support a concern about witness intimidation or safety. *United States v. Barbeito*, 2009 U.S. Dist. LEXIS 102688 (S.D. W.Va. 2009). The third-party-sourced documents are not child

pornography or any other contraband. The government has no basis to claim that the withheld information is privileged (*United States v. Thompson*, 562 F.3d 387 (D.C. Cir. 2009)(work product privilege), patented (stipulated protective order in *United States v. Pani*, 08-CR 40034-FDS), or copyrighted. Unlike, the agreed order entered in *United States v. Gonzalez*, 2009 U.S. Dist. LEXIS 50791 (D.Mass. 2009), there is no personal financial information involved here, such as the credit card or social security numbers of consumers.

The government's unsupported assertion that some part of the third-party-sourced information may be "**potentially** sensitive, confidential, and proprietary" falls far short of good cause. The government asserts that some of the information includes discussion of the computer systems of MIT and JSTOR and security measures. This information is discoverable because it constitutes putative evidence that will be publicly disclosed in this litigation, including a public trial. The Court's September 9, 2011 order allows Mr. Swartz to oppose the government's motion for a protective order but, certainly, nothing in the government's August 12, 2001 letter to defense counsel constitutes good cause to impose a protective order concerning any third-party-sourced information.

4. **Electronically-Stored Information Provided by the Defendant.** The government is withholding and refusing to provide a copy of the electronic data stored in four Samsung hard drives delivered to the Secret Service by Mr. Swartz on June 7, 2011, at the office of undersigned counsel. The government has made no showing of good cause concerning this data which it would not have in its custody and control, but for Mr. Swartz's delivery of it to the government.

5. **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.

6. **Identifications.** Paragraph G of the government's letter provides documents related to an identification procedure involving the use of a photo array but redacts all identifying information concerning the alleged eyewitness on the unfounded ground that the eyewitness has a right of privacy at this stage of the litigation. Rule 16 does not authorize redaction of information from discoverable documents. The purpose of this discovery rule is to enable the defense to move early in the proceeding to suppress eyewitness testimony, if the eyewitness was subjected to suggestive statements or activity by investigating officials. The purpose of the rule is undermined and rendered ineffective if the identity of the alleged eyewitness is withheld, because no effective investigation of the identification can be conducted without identifying information about the alleged eyewitness. Nothing in the government's letter provides any basis for defeating the purpose of the rule.

7. **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.

The government's letter at page 6 discloses that one of its witnesses has publicly-filed criminal charges pending against him or her, but withholds the name of the witness, purportedly on privacy grounds. The government has not disclosed the documents that mention the publicly-filed criminal charge against the witness. It is obliged by rule and by constitutional principles to disclose those documents. There is no legal basis for redacting the documents or withholding the identity of the witness. The purpose of the automatic discovery rule requiring early disclosure of exculpatory evidence is undermined by withholding witness identifying information.

Conclusion. Because the government has no valid basis for having withheld the discoverable information and evidence itemized in this memorandum, Mr. Swartz urges this Court to issue an order compelling the government to provide, or enable the defense to make, bit-by-bit, mirror image copies of native electronic data that constitute the written statements of the defendant, evidence seized by the government as listed in the motion, third-party-sourced evidence including, but not limited to, evidence from MIT and JSTOR, evidence provided to the government by Mr. Swartz, and exculpatory evidence. The order should also compel the government to disclose the complete video

recordings, and identifying information concerning the alleged eyewitness who was exposed to the photo array and the witness who has publicly-filed criminal charges pending against him or her, as well as all documents that mention those criminal charges.

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: September 27, 2011

/s/ *Andrew Good*
Andrew Good

G:\CLIENTS\Swartz, Aaron\Pleadings - Federal Court Case\Defendant's Motion to Compel Discovery dr2.doc