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

Exhibit 1

U.S. Department of Justice

Carmen M. Ortiz
United States Attorney
District of Massachusetts

Main Reception: (617) 748-3100

United States Courthouse, Suite 9200
1 Courthouse Way
Boston, Massachusetts 02210

August 12, 2011

Mr. Andrew Good
Good and Cormier
83 Atlantic Avenue
Boston, MA 02110

Re: United States v. Aaron Swartz
Criminal No. 11-CR-10260

Dear Counsel:

Pursuant to Fed. R. Crim. P. 16 and Rules 116.1(C) and 116.2 of the Local Rules of the United States District Court for the District of Massachusetts, the government provides the following automatic discovery in the above-referenced case:

A. Rule 16 Materials

1. Statements of Defendant under Rule 16 (a)(1)(A) & (a)(1)(B)

a. Written Statements

The defendant's booking sheet and fingerprint card from the Cambridge Police Department are contained on enclosed Disk 5.

There are numerous relevant statements not made to government agents drafted by Defendant Swartz before the date of his arrest contained in electronic media, such as Twitter postings, websites and e-mail. These are equally available to the defendant. Those that the government intends to use in its case-in-chief are available for your review, as described in paragraph A(3) below.

Subject thereto, there are no relevant written statements of Defendant Swartz made

following his arrest in the possession, custody or control of the government, which are known to the attorney for the government.

b. Recorded Statements

The defendant made recorded statements at the time of his booking by Cambridge Police on January 6, 2011. A copy of his booking video is enclosed on Disk 7.

c. Grand Jury Testimony of the Defendant

Defendant Aaron Swartz did not testify before a grand jury in relation to this case.

d. Oral Statements to Then Known Government Agents

Defendant Aaron Swartz made oral statements at the time of the search of his apartment to individuals known to him at the time to be government agents. The only statements made by him then which the government believes at this time to be material are memorialized in the affidavit in support of the search warrant for his office at Harvard, a copy of which affidavit is enclosed on Disk 3.

2. Defendant's Prior Record under Rule 16 (a)(1)(D)

Enclosed on Disk 3 is a copy of the defendant's prior criminal record.

3. Documents and Tangible Objects under Rule 16(a)(1)(E)

All books, papers, documents and tangible items which are within the possession, custody or control of the government, and which are material to the preparation of the defendant's defense or are intended for use by the government as evidence in chief at the trial of this case, or were obtained from or belong to the defendant, may be inspected subject to a protective order by contacting the undersigned Assistant U.S. Attorney and making an appointment to view the same at a mutually convenient time.

Because many of these items contain potentially sensitive, confidential and proprietary communications, documents, and records obtained from JSTOR and MIT, including discussion of the victims' computer systems and security measures, we will need to arrange a protective order with you before inspection. Please review the enclosed draft agreement and let us know your thoughts.

4. Reports of Examinations and Tests under Rule 16 (a)(1)(F)

Enclosed you will find Disks 1, 2, 5 & 6 containing reports of examination of the following:

- 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
- Four Samsung hard drives delivered to the Secret Service by Defendant Swartz and his counsel on June 7, 2011 (Please note that because of the number of files contained on Samsung model HD154UI hard drive, serial number S1Y6J1C2800332, it has not been practicable to date to make a complete file list in an Excel readable format, unlike the other drives.)
- A fingerprint analysis report from the Cambridge Police Department with respect to the Acer Laptop and Western Digital hard drive recovered at MIT
- A supplemental fingerprint analysis report with respect to these items

While not required by the rules, intermediate as well as final forensic reports where available are enclosed for many of the recovered and seized pieces of equipment on Disks 6 and 1, respectively.

B. Search Materials under Local Rule 116.1(C)(1)(b)

Search warrants were executed on multiple pieces of electronic equipment and at multiple locations. Copies of the search warrants, applications, affidavits, and returns have already been provided to you, but are further found on Disk 3.

Four Samsung Model HD154UI hard drives were examined following their consensual and unconditional delivery to the United States Secret Service on June 7, 2011. As an additional precaution, a warrant, enclosed on Disk 3, was also obtained.

C. Electronic Surveillance under Local Rule 116.1(C)(1)(c)

No oral, wire, or electronic communications of the defendant as defined in 18 U.S.C. § 2510 were intercepted relating to the charges in the indictment.

D. Consensual Interceptions under Local Rule 116.1(C)(1)(d)

There were no interceptions (as the term "intercept" is defined in 18 U.S.C. § 2510(4)) of wire, oral, or electronic communications relating to the charges contained in the indictment, made with the consent of one of the parties to the communication in which the defendant was intercepted or which the government intends to offer as evidence in its case-in-chief.

E. Video Recordings

On January 4, 2011 and January 6, 2011, Defendant Aaron Swartz was recorded entering a restricted wiring closet in the basement of MIT's Building 16. Copies of relevant portions of the recordings (where he is seen entering, in, or exiting the closet) are enclosed on Disk 4.

F. Unindicted Coconspirators under Local Rule 116.1(C)(1)(e)

There is no conspiracy count charged in the indictment.

G. Identifications under Local Rule 116.1(C)(1)(f)

Defendant Aaron Swartz was a subject of an investigative identification procedure used with a witness the government anticipates calling in its case-in-chief involving a photospread documented by MIT Police Detective Boulter. Relevant portions of the police report of Detective Boulter and a copy of the photospread used in the identification procedure are enclosed on Disk 3. In both instances, the name of the identifying MIT student has been redacted to protect the student's continuing right to privacy at this initial stage of the case. On page 2 of the Report of Photo Array, USAO-000007, the initials beside each of the enumerated items have been redacted for the same reason.

H. Exculpatory Evidence Under Local Rule 116.2(B)(1)

With respect to the government's obligation under Local Rule 116.2(B)(1) to produce "exculpatory evidence" as that term is defined in Local Rule 116.2(A), the government states as follows:

1. The government is unaware of any information that would tend directly to negate the defendant's guilt concerning any count in the indictment. However, the United States is aware of the following information that you may consider to be discoverable under Local Rule 116.2(B)(1)(a):

- Email exchanges between and among individuals at MIT and JSTOR as they sought to identify the individual responsible for massive downloads on the dates charged in the Indictment. While the defendant has admitted to being responsible for the downloads and produced one copy of most of what was downloaded on these dates, these e-mails reflect JSTOR's and MIT's initial difficulties in locating and identifying him in light of the furtive tactics he was employing. The email exchanges will be made available in accordance with paragraph (A)(3) above.

- Counsel for the government understands that a number of external connections were made and/or attempted to the Acer laptop between January 4, 2011 and January 6, 2011, including from a Linux server at MIT and from China. The Linux server was connected to a medical center at Harvard periodically during the same period. While government

counsel is unaware of any evidence that files from JSTOR were extracted by third parties through any of these connections, the connection logs will be made available to you in accordance with paragraph (A)(3) above.

- An analysis of one of the fingerprints on the Acer laptop purchased and used by the defendant cannot exclude his friend, Alec Resnick. The analysis is being produced for you; see paragraph (A)(4) above.

- While not a defense or material, one or more other people used or attempted to use scrapers to download JSTOR articles through MIT computers during the period of Defendant Swartz's illegal conduct. On the evening of November 29, 2010, the network security team at MIT was contacted and investigated journal spidering occurring on the site of the Institute of Electrical and Electronic Engineers. It was tracked to a group of shared computers on which anyone at MIT can host a virtual machine. It was determined that a virtual machine had been compromised. The user was notified that scripts placed on it were downloading journals from JSTOR, IEEE and APS. The machines were taken offline early the morning of November 30, 2010.

- The login screen on the Acer laptop when observed by Secret Service Agent Pickett on January 4, 2011 identified the user currently logged in as "Gene Host." A user name is different from a host name, and accordingly is similarly immaterial.

2. The government is unaware of any information that would cast doubt on the admissibility of evidence that the government anticipates offering in its case-in-chief and that could be subject to a motion to suppress or exclude.

3. Promises, rewards, or inducements have been given to witness Erin Quinn Norton. Copies of the letter agreement with her and order of immunity with respect to her grand jury testimony are enclosed on Disk 3.

4. The government is aware of one case-in-chief witness who has a criminal record.

Please be advised that one of the government's prospective trial witnesses was the subject of a charge in Somerville District Court in 1998 of being a minor in possession of alcohol and that the case was dismissed the following month upon payment of court costs. The government intends to make no further disclosures with respect to this matter, as the criminal charge could have no possible admissibility under either Fed.R.Crim.P. 609 or 608(b). If you believe you are entitled to additional information, including the identity of the prospective witness, please advise the undersigned, in which event the government will seek a protective order from the court to permit non-disclosure.

5. The government is aware of one case-in-chief witnesses who has a criminal case pending.

Please be advised that one of the government's prospective trial witnesses has pending state charges brought on July 7, 2009, involving the Abuse Prevention Act, Possession of Burglarious Tools, Criminal Harassment, and Breaking and Entering in the Daytime With Intent to Commit a felony. The events underlying the charges arise from the break-up of a personal relationship. The government has withheld the name of the witness and the others involved to protect their privacy, but will make them available along with the police reports in its possession subject to a protective order ensuring that the names, events and reports will not be disclosed publicly until the trial of this case, should the Court determine that a charge or information contained in the police reports is admissible for the purposes of cross-examination.

6. Based on the timeline as the government presently understands it from Officer Boulter's report described in paragraph G above and contained on Disk 3, no named percipient witnesses failed to make a positive identification of the defendant with respect to the crimes at issue. As reflected in the report, three students present when the Acer computer and Western Digital hard drive were recovered from Building 20 by law enforcement stated that they did not see anyone come in and place the computer there. However, as the timeline reflects, this was not a failed identification, but rather that they were not percipient witnesses to the event which had occurred earlier.

I. Other Matters

The government has preliminary analysis notes prepared at Carnegie Mellon of certain code and files contained on the Acer Laptop, as referenced on Page 2 of SA Michael Pickett's Forensic Cover Report contained on Disk 1. While these are not encompassed by Rule 16 (a)(1)(F) (formerly 16(a)(1)(D)), the government will make these available for review as described in section (A)(3), above, subject to the same procedures proscribed for preliminary transcripts in Local Rule 116.4 (B)(2).

Your involvement in the delivery of four hard drives containing documents, records and data obtained from JSTOR creates potential issues in this case under the Rules of Professional Conduct, as I am sure you are aware. To avoid the potential for those issues under Rule 3.7 in particular, we propose a stipulation from your client that the hard drives were from him, thus taking you out of the middle and rendering the origin an uncontested issue under the Rule. This stipulation would be without prejudice to all arguments on both sides as to the admissibility of the drives and their contents at any proceeding.

The government is aware of its continuing duty to disclose newly discovered additional evidence or material that is subject to discovery or inspection under Local Rules 116.1 and 116.2(B)(1) and Rule 16 of the Federal Rules of Criminal Procedure.

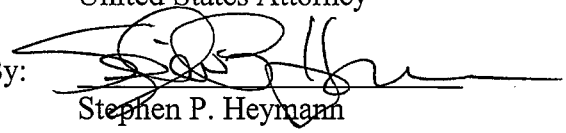
The government requests reciprocal discovery pursuant to Rule 16(b) of the Federal Rules of Criminal Procedure and Local Rule 116.1(D).

The government demands, pursuant to Rule 12.1 of the Federal Rules of Criminal Procedure, written notice of the defendant's intention to offer a defense of alibi. The time, date, and place at which the alleged offenses were committed is set forth in the indictment in this case a copy of which you previously have received.

Please call the undersigned Assistant U.S. Attorney at 617-748-3100 if you have any questions.

Very truly yours,

CARMEN M. ORTIZ
United States Attorney

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

enclosures