UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES	)	
v.	)	No. 11-10260-NMG
AARON SWARTZ	)	

DEFENDANT AARON SWARTZ'S MOTION FOR DISCOVERY

On May 8, 2012, defendant Aaron Swartz sought from the government 21 enumerated categories of discovery from the government. *See* Exhibit A, submitted herewith. That request was followed by a letter dated May 10, 2012, outlining the bases for the requests made in the earlier letter. *See* Exhibit B, submitted herewith. Following discussions by the parties conducted in good faith to eliminate and/or narrow the areas of dispute, the government responded to Swartz's discovery requests on May 18, 2012. *See* Exhibit C, submitted herewith. This motion requests that the government be ordered to provide Swartz with the discovery which it has declined to produce: that described in paragraphs 1, 4, 6, 12, 15, and 20 of Swartz's May 8, 2012, discovery request letter.

I. PARAGRAPH 6.

This paragraph requested that the government provide "[a]ny and all notes and reports provided to USSS or USAO by CERT in relation to their forensic analysis of the ACER laptop, or of any analysis of any other evidence including but not limited to the PCAP log information sent to CERT by the USSS for analysis." "CERT" in this request refers to the Carnegie Mellon computer response team which provides assistance to the USSS with complex computer and internet issues.

In this case, CERT conducted analyses, which it provided to the United States Attorney's Office, of MIT computer/internet information relating to Swartz's alleged use of the MIT system and/or of certain computers or hard drives which the government associates with Swartz. Information received in discovery indicates that the flow traffic on MIT's network was being contemporaneously uploaded to the CERT "dropbox."The government has declined to provide these reports and other information on the ground that no CERT personnel will be appearing as expert witnesses at the trial of this case and that, if they do, such discovery should be subject to the separate schedule for the disclosure of reports of experts rather than to the obligations relating to disclosure of scientific results or tests. That fact, however, does not eliminate the defendant's entitlement to this information. Swartz is entitled to the production of reports of scientific tests under Fed. R. Evid. 16(a)(1)(F), which entitles the defendant to the "results or reports" of "any scientific test or experiment" if the item is in the possession of the government – as it is here – and if the item is material to the preparation of the defense *or* the government intends to us the item in its case-in-chief at trial. Rule 16(a)(1)(F) encompasses forensic examination of computer/internet data or information. *See, e.g., United States v. Pires*, 2009 WL 2176664 at *1 (D.Mass. July 22, 2009); *United States v. Robinson*, 2006 WL 468298 at *4 (N.D.Tex. Feb. 28, 2006). Here, the requested information is material to the preparation of Swartz's defense and to Swartz's potential ability to file a particularized motion to suppress asserting violations of 18 U.S.C. §2510 *et seq.* and/or the Fourth Amendment.

II. PARAGRAPH 12.

This paragraph requested that the government provide:

> As to the ACER laptop: the dates of any searches (defined as any attempt to see any information contained on the computer that would not be visible without touching the computer in any way including but not limited to any port scan of the computer, any imaging

> of the laptop or any portion of its contents, any powering or opening of any file or folder or data contained in the laptop, any touching of a key or moving of a mouse so as to put in view new information, and any analysis or review by CERT or USSS of any of the contents of the laptop whether obtained remotely, by a physical search, or by a search of an image of the laptop), the identity of each individual who conducted any search of the laptop computer, the date of such search and the legal basis for each such search.

The government has provided Swartz with the February, 2011, search warrant authorizing the search of an ACER laptop alleged to have been used by Swartz in relation to the events which are the subject of the indictment in this case. However, Swartz has information indicating that the government attempted to gain access to the contents of the laptop and/or to modify the condition of the ACER laptop on January 6, 2011, the date of its seizure, and possibly at other times prior to the execution of the search warrant. Moving a mouse or touching a key on a computer which reveals information that was not in plain view constitutes a search which may not be lawfully conducted under the Fourth Amendment in the absence of a valid warrant. *See, e.g., United States v. Musgrove*, 2011 WL 4356515 at *15 (E.D.Wis. September 16, 2011); *see also Arizona v. Hicks*, 480 U.S. 321 (1987). The requested information is critical to Swartz's ability to prepare a particularized motion to suppress unlawfully obtained evidence or other information if such incursions or attempted incursions into the contents of the laptop were made in the absence of a validly issued search warrant.

III. PARAGRAPH 15.

This paragraph asked the government to "identify the origin of any and all statements of Aaron Swartz including but not limited to emails, text messages, chats, documents, memoranda or letters, i.e., to identify the source from which each statement was received and the legal procedure used to obtain each such statement of the defendant." Swartz has received in discovery internet

memoranda and chats purporting to be from him. For example, the discovery contains a number of chats on googlegroups.com which contain entries which facially indicate that Swartz was a participant in the communications. The discovery also contains a number of emails which on their faces indicate that they were either to or from Swartz. Swartz requires the additional information requested – the source of these statements and the procedure used by the government to obtain them – to enable him to move to suppress such statements if grounds exist to do so, which he cannot determine without the requested information. *See* Fed. R. Crim. P. 12(b)(4).

IV. PARAGRAPHS 1, 4, 20.

These paragraphs request information relating to grand jury subpoenas. Paragraph 1 requested that the government provide "[a]ny and all grand jury subpoenas – and any and all information resulting from their service – seeking information from third parties including but not limited to Twitter. MIT, JSTOR, Internet Archive that would constitute a communication from or to Aaron Swartz or any computer associated with him." Paragraph 4 requested "[a]ny and all SCA applications, orders or subpoenas to MIT, JSTOR, Twitter, Google, Amazon, Internet Archive or any other entity seeking information regarding Aaron Swartz, any account associated with Swartz, or any information regarding communications to and from Swartz and any and all information resulting from their service." Paragraph 20 requested "[a]ny and all paper, documents, materials, information and data of any kind received by the Government as a result of the service of any grand jury subpoena on any person or entity relating to this investigation."

Swartz requests this information because some grand jury subpoenas used in this case contained directives to the recipients which Swartz contends were in conflict with Rule 6(e)(2)(A), *see United States v. Kramer*, 864 F.2d 99, 101 (11th Cir. 1988), and others sought certification of

the produced documents so that they could be offered into evidence under Fed. R. Evid. 803(6), 901. Swartz requires the requested materials to determine whether there is a further basis for moving to exclude evidence under the Fourth Amendment (even though the SCA has no independent suppression remedy).

The Fourth Amendment "provides protection against a grand jury subpoena too sweeping in its terms "to be regarded as reasonable.'" *United States v. Dionisio*, 410 U.S. 1, 11 (1973), *quoting Hale v. Henkel*, 201 U.S. 43, 76 (1906). *See United States v. Calandra*, 414 U.S. 338, 346 (1974)("A grand jury's subpoena duces tecum will be disallowed if it is 'far too sweeping in its terms to be regarded as reasonable' under the Fourth Amendment"); *In re Horowitz*, 482 F.2d 72, 79 (2d Cir. 1973)("the Constitution undoubtedly protects against overly broad *subpoenas duces tecum*"); *In re Eight Grand Jury Subpoenae Duces Tecum*, 701 F.Supp. 53, 55 (S.D.N.Y. 1988)(grand jury "may not issue a subpoena so broad as to impinge unreasonably on legitimate fourth amendment rights"); *In re Grand Jury Subpoenas Served Feb. 27, 1984*, 599 F.Supp. 1006, 1017 (E.D. Wash. 1984)("There is no doubt that a grand jury subpoena *duces tecum* must pass constitutional muster"). Swartz retains a reasonable expectation of privacy in his emails and chat communications even though they are in the hands of a third party internet service provider. *See United States v. Warshak*, 631 F.3d 266, 283-87 (2010).

Moreover, defendant believes that the items would not have been subpoenaed by the experienced and respected senior prosecutor, nor would evidentiary certifications have been requested, were the subpoenaed items not material to either the prosecution or the defense. Defendant's viewing of any undisclosed subpoenaed materials would not be burdensome, and disclosure of the subpoenas would not intrude upon the government's work product privilege, as the

subpoenas were served on third parties, thus waiving any confidentiality or privilege protections.

Respectfully submitted,
By his attorney,

/s/ Martin G. Weinberg
Martin G. Weinberg
20 Park Plaza, Suite 1000
Boston, MA 02116
(617) 227-3700 (tel.)
(617) 338-9538 (fax)
owlmgw@att.net

CERTIFICATE OF SERVICE

I, Martin G. Weinberg, hereby certify that on this 1st day of June, 2012, a copy of the foregoing document has been served via the Court's ECF system on all registered participants, including Stephen P. Heymann, AUSA.

/s/ Martin G. Weinberg

Martin G. Weinberg