UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

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

Government's Response to Defendant Aaron Swartz's Motion for Discovery

The government has provided extensive discovery in this case, voluntarily going well beyond the requirements of Federal Rule of Criminal Procedure 16, the Local Rules and the Constitution in order to give the defendant and his counsel a clear view of the investigation that preceded the defendant's arrest. The defendant has responded with four very broad discovery requests effectively seeking access to the entirety of the government's investigative files and work product. These requests should be denied. The Supreme Court has explicitly "rejected the notion that a 'prosecutor has a constitutional duty routinely to deliver his entire file to defense counsel.'" *Arizona v. Youngblood*, 486 U.S. 51, 55 (1988) (quoting *United States v. Agurs*, 427 U.S. 97, 111 (1976)). *See also Moore v. Illinois*, 488 U.S. 786, 795 (1972) ("We knew of no constitutional requirement that the prosecution make a complete and detailed accounting to the defense of all police investigatory work on a case.")

Background Common to Defendant's First Two Requests

The Indictment charges that:

Between September 24, 2010 and January 6, 2011, Swartz contrived to:

a. break into a computer wiring closet at MIT;

b. access MIT's network without authorization from a switch within that closet;

c. connect to JSTOR's archive of digitized journal articles through MIT's computer network;

d. use this access to download a major portion of JSTOR's archive onto his computers and computer hard drives;

e. avoid MIT's and JSTOR's efforts to prevent this massive copying, measures which were directed at users generally and Swartz's illicit conduct specifically; and

f. elude detection and identification;

all with the purpose of distributing a significant portion of JSTOR's archive through one or more file-sharing sites.

Indictment (Docket #2) at ¶ 11.

Swartz used an ACER laptop, among other equipment, to access MIT's computer network and to steal JSTOR's files. Having searched for the source of the illegal JSTOR downloads for months, MIT finally located the laptop on January 4, 2010, in a restricted wiring closet in the basement of an MIT building hidden under a box and hard-wired into a computer switch. MIT contacted local and federal law enforcement officers and began monitoring what the then-unidentified hacker's computer was doing on their network. The computer logs of these activities were subsequently provided to the United States Secret Service.

When called in, law enforcement officers photographed the scene and lifted fingerprint impressions from the computer. They also examined the computer itself and determined it was password protected, prohibiting them from taking forensic steps only possible before a computer is turned off.

Swartz was identified as the unknown hacker and thief after he was videotaped returning to the closet twice, on one occasion trying to shield his identity by holding a bicycle helmet over

his face. On the second occasion, he moved the ACER laptop from the restricted basement wiring closet to another location at MIT, where it was ultimately recovered by law enforcement officers. Swartz was arrested a short time later after fleeing police.

I. Paragraph 6[1]

The defendant has requested first that the government provide "[a]ny and all notes and reports provided to USSS or USAO by CERT in relation to the forensic analysis of the ACER laptop, or any analysis of any evidence including but not limited to the PCAP log information sent to CERT by the USSS for analysis." The Court should deny this request because it seeks expert opinions long in advance of the schedule previously agreed upon by the parties and ordered by the Court, and also because it seeks materials covered by the work product privilege.

The United States Secret Service obtained a warrant to search the laptop, and then performed a forensic examination of the computer. To obtain expert opinions of both the contents of the laptop and the logs of its activities on MIT's network, the Secret Service turned to CERT. CERT is Carnegie Mellon University's Computer Emergency Response Team, which assists the Secret Service with complex computer matters. CERT identified files from the laptop's hard drive that it considered potentially material to the prosecution of this case. It also provided preliminary opinions about how to interpret software code found on the laptop.[2]

The government has not determined who it will call as an expert at trial. Nor has the government asked any expert to prepare a final expert report concerning the contents of the

[1] For clarity, the government refers to the defendant's requests using the same subheadings used in the Defendant's motion.

[2] A similar investigative pattern was followed with respect to a number of hard drives and a USB drive seized during the investigation.

laptop or anything else.

CERT's margin descriptions and other preliminary interpretations of software and files on the seized laptop computer are not discoverable. *See United States v. Iglesias,* 881 F.2d 1519, 1523 (9th Cir. 1989) (holding that government satisfied its obligation to produce results and reports under Fed. R. Crim. P. 16 by turning over lab report determining substance to be 54.9% heroin and was not required to contemporaneously turn over log notes, protocols, and other internal documents of chemist because they did not have the requisite formality or finality to be considered as either a "report" or "result"); *United States v. Wilkerson*, 189 F.R.D. 14, 15-16 (D.Ma. 1999) (Collings, J.) (holding that records, notes and documentation concerning drug testing of controlled substance were not results or reports of test under Rule 16). Fed. R. Crim. P. 16 (a)(2) expressly states that the rule, "does not authorize the discovery or inspection of reports, memoranda, or other internal documents made by an attorney for the government or other government agent in connection with investigating or prosecuting the case."

Even were the margin descriptions and preliminary interpretations sufficiently formal or final to be considered "reports" or "results," they are not discoverable at this particular time. In *U.S. v. Pires*, 2009 WL 2176664 (D. Mass. July 22, 2009), relied on by the defendant, Judge Zobel ruled on two separate arguments by a defendant that he should be provided the results of the examination of his computer's contents during discovery. She required the government to describe substantively the *contents* of evidence found on a computer on which it intended to rely pursuant to Rule 16(a)(1)(F) (reports of examinations), which is timed earlier in the discovery process. Then she obligated the government to produce *interpretations* of and *inferences* from that evidence which it intended to elicit from its experts pursuant to Rule 16(a)(1)(G) (expert

opinions), which is timed later in the process.

The government has previously provided the defendant a complete copy of the ACER laptop's hard drive and a forensic report of its examination. It does not object, in light of *Pires*, to early identification of files, records and software code which it has determined to date may be material and offered as evidence at trial. In keeping with the distinction drawn in *Pires*, this Court should deny the defendant's motion to the extent that it seeks any opinions drawn about the meaning of that source code provided to the U.S. Attorney's Office or the United States Secret Service by CERT. To do otherwise, would provide raw investigative work product to the defendant. It also would completely undermine the schedule of expert disclosure explicitly agreed upon by the parties, submitted by them jointly to the Court, and directed in the Interim Status Reports. *See*, *e.g.*, Interim Status Report, May 23, 2012 (Docket # 38) at ¶ 6.

II. Paragraph 12

In his next request, the defendant seeks the dates and identities of each person who ever touched the ACER laptop and a written legal justification for that person doing so. The defendant's request should be denied. The government not only has fully complied with its obligations under Local Rule 116.1(c)(1)(B) concerning the production of search materials, but also, well beyond that.

Local Rule 116.1(a)(1)(B) details the government's obligations in this district with respect to search materials. The government has greatly exceeded compliance with its discovery obligation with respect to searches. It has, of course, provided copies of all search warrants in this case. But, beyond that, it has provided the email traffic at MIT reflecting investigative steps being taken by them, all police and agent reports from the date of the ACER's discovery to its

seizure and the defendant's arrest, and even an internal U.S. Attorney's Office email containing facts concerning the handling of the ACER laptop upon its discovery which, upon initial review, government counsel did not see contained in other reports being provided to the defendant.

The defendant claims that additional discovery is necessary because even touching a computer key may be an unlawful search without a warrant. While he might be able to argue this extreme claim if the computer had been touched in defendant's apartment or office, he lost all reasonable expectation of privacy in the computer once he broke into MIT's wiring closet to steal JSTOR's files through MIT's hacked network and hid the computer under a box.

A trespasser who conceals personal items in someone else's property cannot assert the Fourth Amendment as a basis for challenging the search. *United States v. Terry*, 2001 WL 496630 at *2, n.5 (S.D.Ga. 2007); *United States v. Pitt*, 717 F.2d 1334-37 (11th Cir. 1983) (holding defendant lacks standing where he was a trespasser "who assumed to lock the door which he had no legal right to lock); *United States v. Sanchez*, 635 F.2d 47, 64 (2nd Cir. 1980) ("[A] mere trespasser has no Fourth Amendment protection in premises he occupies wrongfully."); *United States v. Hightower*, 1987 WL 44897 at * 2 (6th Cir. Sept. 28, 1987) (holding that country club member who placed lock on a locker that he had not been assigned and on which he had not paid the annual rental fee "was in essence a trespasser" whose expectation of privacy was not legitimate); *see* 6 Wayne R. LaFave, Search and Seizure § 11.3(d), at 185 n.234 (4th ed. 2004) ("[A] trespasser certainly does not have standing"); *Rakas v. Illinois*, 439 U.S. 128, 143 (1987) ("Obviously, ... a 'legitimate' expectation of privacy by definition means more than a subjective expectation of not being discovered. A burglar plying his trade in a summer cabin during the off-season may have a thoroughly justified subjective

expectation of privacy, but it is not one which the law recognizes as 'legitimate.' His presence ... is 'wrongful'; his expectation is not 'one that society is prepared to recognize 'reasonable.'").

The defendant already has the facts and evidence to determine whether he has grounds to file a motion to suppress. Ordering that the government provide a written legal justification for steps taken by it during an investigation is outside the scope of pretrial discovery. The defendant's request that the government prepare further documentation of the handling of his ACER laptop and its legal justification for doing so is wholly without merit and should be denied.

III. Paragraph 15

In Paragraph 15, the defendant would require the government to identify the origin of any and all statements of Aaron Swartz in its possession and the legal procedure used to obtain the statements. All of the emails, text messages, chat sessions, and documents containing statements provided by the defendant relevant to this case were obtained either from individuals with whom the defendant communicated or from publicly available websites stored on the Internet. No emails, texts messages, chat logs, or documents were obtained from Internet service providers using orders under 18 U.S.C. 2703(d). As previously represented to defense counsel, there was no court-authorized electronic surveillance in this case.

The government objects to further particularization at this time. First, further particularization would identify witnesses long in advance of the time prescribed by the Local Rules. Second, as with his claim that he is entitled to an immediate written legal justification for each touching of his laptop, his demand for a written legal justification for each occasion during an investigation the government obtained a copy of something he wrote is outside the

scope of pretrial discovery.

IV. Paragraphs 1, 4, 20

Lastly, the defendant seeks any and all grand jury subpoenas and any and all information resulting from them, in essence, complete and open access to all aspects of the government's investigative files, including the statements of all witnesses before the grand jury and all documents and records obtained during the course of the investigation. Both Federal Rule of Criminal Procedure 16 and Local Rules 116.1-116.2 dispositively reject the concept of "open file" discovery in the federal courts. The defendant's request in this regard should be denied.

As a pre-requisite, the defendant has not established standing to move to suppress the subpoenas issued in the course of the grand jury investigation. "When those seeking to challenge a subpoena directed to a third party claim standing to raise a Fourth or Fifth Amendment issue, they must establish either the existence of a privileged relationship or of a legitimate property or privacy interest in the documents possessed by the third party." *In re Grand Jury Proceedings (Diamonte),* 814 F.2d 61, 66 (1st Cir. 1987).

The defendant instead moves directly to three vague justifications for his request. First, he suggests that some unspecified grand jury subpoenas used in this case contained "*directives*" to the recipients in conflict with Rule 6(e)(2)(A), which states that "no obligation of secrecy may be imposed on any person except in accordance with Rule 6(e)(2)(B)." None of the subpoenas used in this case contained a "*directive*" to recipients of secrecy. Most were accompanied by a letter containing a *request* consistent with controlling First Circuit precedent, stating in pertinent part:

> We request that you not disclose the existence of the subpoena, or the fact of your compliance with it, to anyone. *While you are not required to comply with this*

> *request, any such disclosure could impede the investigation and interfere with the enforcement of federal criminal law.*

The First Circuit has expressly approved such requests and expressions of opinion: "The government is free to express its beliefs about the impact of any disclosure, provided it makes clear that the law does not require non-disclosure." *In re Grand Jury Proceedings (Diamonte),* 814 F.2d at 70.

Second, the defendant urges, without any factual evidence or basis, that some of the government's grand jury subpoenas may have been "too sweeping in terms 'to be regarded as reasonable.'" There is no basis for the defendant getting unprecedented access to all of the government's grand jury subpoenas, grand jury transcripts, and documents and records produced by witnesses in response to those subpoenas based solely on the defendant's bald conclusory assertion that some might have been overly broad.

Finally, with a coy use of the word "material," the defendant argues that he is entitled to the entire investigative file because a senior prosecutor would not have sought the materials during an investigation were they not material to the prosecution or the defense. As complimentary as the apparent tautology may be, it fails in two, independent regards.

During an investigation, the government subpoenas records and obtains testimony before the grand jury that in good faith it prospectively believes may be relevant to the investigation. Not being omniscient, records and testimony often turn out not to be material to the prosecution or defense of the case as charged. They lead to investigative dead ends or the production of records or testimony which upon analysis turn out to be off point. Requiring the government to produce all of the government subpoenas, all grand jury testimony that followed, and all of the documents and records which were received would cause problems that the rules were designed

to prevent. It would result in disclosure of witnesses before the grand jury contrary to the specific intent of Fed. R. Crim. P. 6(e)(2), the transfer of records and documents to the defendant belonging to otherwise uninvolved third parties, and the disclosure of the work product and thought processes of the U.S. Attorney's Office during its investigation.

Furthermore, the request seeks to sidestep specific timing requirements created by statute and the local rules. For example while grand jury transcripts may be material both to the prosecution and the defense, the Jencks act and Local Rule 117.1(a)(5) reflect the determination that they need be provided only as trial approaches, and not before.

For these reasons, the defendant's over-reaching requests that he be provided all grand jury subpoenas and what was obtained pursuant to those subpoenas should be denied.[3]

Respectfully submitted,

Carmen M. Ortiz
United States Attorney

By: */s/ Stephen P. Heymann*
STEPHEN P. HEYMANN
SCOTT L. GARLAND
Assistant U.S. Attorneys

Date: June 22, 2012

[3] As stated earlier, there were no applications pursuant to 18 U.S.C. §2703(d) for records from electronic communications service providers in this case. Accordingly, to the extent the defendant's request seeks these applications and orders, the defendant's request is moot.

CERTIFICATE OF SERVICE

I hereby certify that this document filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF).

/s/ Stephen P. Heymann
STEPHEN P. HEYMANN
Assistant U. S. Attorney

Date: June 22, 2012