UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

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

MOTION TO SUPPRESS ALL FRUITS OF WARRANTLESS SEARCHES CONDUCTED FROM JANUARY 4, 2011, TO JANUARY 6, 2011, AND INCORPORATED MEMORANDUM OF LAW (MOTION TO SUPPRESS NO. 2)

Now comes the defendant Aaron Swartz and respectfully moves that this Honorable Court suppress as evidence at the trial of this case all evidence derived from unlawful warrantless searches of, and unlawful interceptions of electronic communications/data to and from, an ACER netbook belonging to him, from January 4, 2011, through January 6, 2011, and all derivative fruits thereof.

As reason therefor, defendant states:

1. He had a reasonable expectation of privacy in his netbook and in the communications/data flowing to and from it.[1]

2. From January 4, 2011, through January 6, 2011, MIT personnel, Secret Service agents, and Cambridge police unlawfully searched his ACER netbook and intercepted communications/data flowing to and from the netbook, without either a search warrant or an order authorizing the interception of electronic communications under Title III.

3. To the extent that such searches/interceptions were carried out by MIT personnel, they were acting as government agents, and the requirements of the Fourth Amendment apply.

[1] All averments herein regarding Swartz's ownership and possession of the ACER laptop and the hard drive are made pursuant to the protections provided by *Simmons v. United States*, 390 U.S. 377, 392-94 (1968).

4. The evidence, along with all derivative fruits thereof, must, therefore, be suppressed.

THE DEFENDANT REQUESTS A HEARING ON THE WITHIN MOTION.

LOCAL RULE 7.1(A)(2) STATEMENT

The undersigned counsel has conferred with AUSA Stephen Heymann. The government opposes the suppression remedies sought and will respond to defendant's request for a hearing in its response to the motion.

MEMORANDUM OF LAW

I. FACTUAL BACKGROUND.

From September 27, 2010, until January 4, 2011, MIT personnel conducted an investigation into the downloading of large quantities of material from JSTOR, an online archive which provides access to academic journals.[2] Timeline of events related to JSTOR downloading incident: 9/26/10-1/6/11 ("Timeline"), Exhibit 1 at 1-5. On January 4, 2011, Dave Newman, MIT Senior Network Engineer, located an ACER netbook in a data room in the basement of an MIT building, which Newman believed was the computer being used to download journal articles from JSTOR. Timeline at 6. Newman, in consultation with Paul Acosta, MIT Manager of Network Operations, decided to leave the netbook physically undisturbed and instead to institute a "capture" of the network traffic to and from the netbook, which was done via Newman's laptop, which was connected to the netbook and which intercepted communications coming to it. *Id.*; US Secret Service Investigative Report ("Investigative Report"), Exhibit 15 at 2. These interceptions were commenced without a warrant or other judicial process. At 11:00 am, Captain Jay Perault of the MIT police arrived, along with

[2] The events which occurred during this time period are further addressed in a separate motion to suppress. *See* Motion to Suppress All Fruits of Interceptions and Disclosures of Electronic Communications and Other Information by MIT Personnel in Violation of the Fourth Amendment and the Stored Communications Act and Incorporated Memorandum of Law. The events relevant to this motion began on the morning of January 4, 2011.

Det. Joseph Murphy of the Cambridge Police Department and Secret Service S/A Michael Pickett, who told MIT personnel that he handled computer forensics for the Secret Service. *Id.*; Investigative Report at 1. It was decided, "*at the recommendation of Michael Pickett*," that the netbook would be left in place, with MIT continuing to monitor the traffic to and from it, and that video surveillance would be set up in the data room to assist in identifying "the suspect." Timeline at 6 (emphasis added). *See* Grand Jury Testimony of Det. Joseph Murphy, July 14, 2011, Exhibit 16 at 66 ("Murphy Grand Jury")(Murphy testified that after learning that MIT had begun the packet capture, "we" told MIT personnel that "[w]e'd like you to keep this running" and, ultimately, "we end up persuading them to leave that on the system"); Email from Ellen Duranceau, MIT Program Manager of Scholarly Publishing and Licensing, to Ann Wolpert, MIT Director of Libraries, January 4, 2011, 3:35 pm, Exhibit 17 ("the offending computer has been found, on the MIT campus. *The police would like to leave it up and running for a couple of days while the investigation continues*" (emphasis added)). Neither S/A Pickett nor Det. Murphy applied for or received a Title III warrant authorizing the interception of electronic communications or were in any way authorized by judicial process to direct and persuade MIT personnel to intercept communications and other data flowing to and from the ACER netbook between 11:00 am on January 4, 2011, and the time of the seizure of the ACER on January 6, 2011.

During the morning of January 4, 2011, the search participants observed that "the netbook [was] still reaching out to JSTOR and downloading journals." *Id.* A warrantless NMap search[3] of the netbook showed that ports 22 and 8092 – ports associated with remote access – were open. Timeline at 7; Investigative Report at 1. The laptop was also physically manipulated and

[3] NMap is a sophisticated port-scanning software that can determine a large amount of information about a computer, including which of a computer's ports are open, the computer's operating system, and which of thousands of services and protocols the computer is using. *See http://en.wikipedia.org/wiki/Nmap* (last visited Sept. 19, 2012).

fingerprinted without a warrant by law enforcement officers. The outside of the netbook was examined, including picking it up and manipulating it. *See* Exhibit 18. The netbook was opened, and the computer screen which showed the operating system being used and the log-in screen which showed a computer name of "ghost-laptop" with the user name "Gene Host" were accessed and photographed. *See* Exhibit 19. The log-in screen required a password, and all efforts to bypass it were unsuccessful. Email from S/A Pickett to AUSA Adam Bookbinder, January 5, 2011 ("Pickett 1/5/11 email"), Exhibit 20 at 1. In addition, the closed, hard-shell case containing the hard drive was fingerprinted; the case was opened, and the hard drive, which law enforcement believed was being used to store the downloaded data, was examined and separately finger printed. *See* Exhibit 21. The opening of the hard drive case and examination of the case and its contents were all done by law enforcement officers on January 4, 2011, without a warrant or any other judicial process.

Newman, Acosta, and S/A Pickett, along with Mike Halsall, MIT Senior Network & Information Security Analyst, continued to physically monitor the netbook until 2:30 pm. Timeline at 7. During that time "strategy [was] determined for continual monitoring of traffic to/from the netbook." *Id.* After the MIT General Counsel's office approved the disclosure of information to law enforcement agents even in the absence of a warrant or process complying with the Stored Communications Act ("SCA"), 18 U.S.C. § 2701 *et seq.* (and in contravention of MIT's published policies of only disclosing such information after receipt of such process), and at a time when MIT personnel were acting as government agents, Halsall gave S/A Pickett historical network flow data relating to two IP addresses associated with the netbook from December 14, 2010, up to that date,[4] and DHCP log information for computers using the MIT network as "ghost macbook" and "ghost

[4] Network flow data shows connections made between computers and the amount of information transmitted. It shows the start and stop time of a connection, the source IP address, the IP address of the website contacted, source and destination port numbers, and the number of bytes of information transmitted.

laptop" for time periods including September and October of the previous year. *Id.*; Investigative Report at 3.[5] The scene was "restored to the way it was found." Timeline at 7. At 3:50 pm on January 4, 2011, Ellen Duranceau sent an email to Brian Larsen at JSTOR stating that she had "just had an update from Mike Halsall of our network security team. *The investigation has moved beyond MIT and is now being handled by law enforcement*, including federal law enforcement . . . . The machine through which the abuse occurred is still live, pending further steps in the investigation." Exhibit 22 (emphasis added). At 3:26 pm, an individual, later identified as Swartz, was observed via the video surveillance to enter the data room and replace the external hard drive attached to the netbook with a different one. Timeline at 7.

S/A Pickett left the MIT campus at 4 pm on January 4, and Newman waited to hear from him regarding "where to put the captured network traffic." Timeline at 7. Thereafter, Pickett contacted the CERT Coordination Center at the Software Engineering Institute at Carnegie Mellon University[6] and received instructions regarding how to upload the network flow and DHCP log data to the CERT drop box. Investigative Report at 3. S/A Pickett authored an email at 6:46 pm on January 4, 2011, stating that "[t]he flow traffic is currently being uploaded to the CERT dropbox." Exhibit 23.

On January 5, 2011, Ellen Finnie Duranceau, MIT Program Manager of Scholarly Publishing and Licensing, took notes of a conversation with Halsall in which she indicated that the netbook was "left in place to capture traffic" because law enforcement "want[ed] to find intent + motive." Exhibit

---

[5] "DHCP" stands for Dynamic Host Configuration Protocol. DHCP assists with the assignment of IP addresses to computers on networks. When a computer joins a network, the computer issues a DHCP request on the network, which asks a DHCP server on the network to provide an IP address to the requesting computer. Part of the information contained in this request is the MAC (Media Access Control) address which is a unique identifier of the network card contained in the computer requesting an IP address. The DHCP logs provide, therefore, significant information in addition to simply the IP addressed used by the computer in question.

[6] CERT has a longstanding and ongoing relationship with the Department of Justice, including the Secret Service, providing technological support for DOJ criminal investigations.

24 at 2. Those same notes stated that it was "now a Federal case" and that everything that had been provided was done "by choice," and not pursuant to a subpoena. *Id.* at 3. Also on January 5, 2011, Newman emailed S/A Pickett at 5:02 pm, stating: "I have collected about 70G of network traffic so far with about 98% of which is the JSTOR journal downloads. . . *I was just wondering what the next step is*." Exhibit 25 ("Email chain") at 2 (emphasis added).[7] The next morning, January 6, 2011, at 9:37 am, Perault sent an email to Newman, S/A Pickett, and Det. Murphy suggesting that the netbook and hard drive be taken offline and asking if the hard drive should be "printed," *i.e.*, imaged. *Id.* S/A Picket responded, agreeing that the netbook should be taken offline and imaged. *Id.* However, he recommended that the video surveillance be maintained because he believed that whoever was using it would return once he noticed that the netbook was offline. Email chain at 1. There was no consideration in any email or report of seeking a judicial warrant for the ongoing interceptions of communications that were being diverted onto and copied on Newman's computer or any consideration of whether judicial process was required for the real-time monitoring of MIT's DHCP logs to identify whether and when the ACER netbook was moved or its connection to the MIT network altered. Given the ongoing video surveillance of the laptop – and the known practice of the owner to return to the data room to swap external hard drives – it cannot be contended that the purpose of the ongoing interceptions of data or the decisions to image the ACER were made to identify the owner rather than for purely law enforcement purposes.

At 12:32 pm on January 6, 2011, an individual later identified as Swartz was observed via video surveillance to enter the data room, remove the netbook and hard drive, and place them in his backpack. Timeline at 7; Investigative Report at 3. Swartz was arrested shortly thereafter; his

[7] The network traffic being intercepted and copied without a warrant was the content of the data or emails or communications between the ACER netbook and third parties, including, but not limited to, JSTOR.

backpack was searched, but the netbook was not there. Investigative Report at 3. When Halsall checked the DHCP logs for computer registrations using the word "ghost" later that afternoon, he observed that the netbook was still active on the MIT network using the same MAC address it had used on January 4, 2011. The netbook was traced to the fifth floor of the Student Center. S/A Pickett was notified and met Halsall at the Student Center. They located the netbook and external hard drive neatly placed under a table, connected to the MIT network. S/A Pickett examined the netbook, which appeared to be frozen halfway in the shutdown state. Attempts were made by the Secret Service to access a terminal on the machine but were unsuccessful; "[i]t was determined it would not be possible to conduct live forensics or capture a snapshot of the memory of the computer in its current state." Investigative Report at 3. The laptop and hard drive were again fingerprinted on January 6, 2012. The laptop and hard drive were then seized and turned over to MIT police. Timeline at 10; Investigative Report at 3. In a January 8, 2011, email from Halsall to Mark Sillis, Halsall's supervisor, discussing Swartz's movements on January 6, 2011, Halsall stated that he had been "gathering up all the stuff for Pickett." Exhibit 26. In a separate email from Halsall to S/A Picket on January 8, 2011, Halsall told Pickett that he "hop[ed] to have the pcap/flows/videos/logs all in by to me Monday, possibly sooner – if you don't already have a copy of the video or pcap [packet capture], I'll make sure you get one." Exhibit 2.

At no time before or during these events was Title III authorization sought for the interception of electronic communications to or from the netbook. No warrant (not even a "sneak and peek" warrant pursuant to 18 U.S.C. §3103a which would have preserved the secrecy of the ongoing efforts to identify the owner of the netbook) to search the netbook or the external hard drive, both of which were seized on January 6, 2011, was obtained until February 9, 2011. Even then, the warrant was not executed, necessitating a reapplication for a search warrant, which was again issued

on February 24, 2011.

II. SWARTZ HAD A REASONABLE EXPECTATION OF PRIVACY IN THE NETBOOK AND EXTERNAL HARD DRIVE.

"Courts routinely recognize that individuals possess objectively reasonable expectations of privacy in the contents of their computers." *United States v. Howe*, 2011 WL 2160472 at *7 (W.D.N.Y. May 27, 2011), adopted 2012 WL 1565708 (W.D.N.Y. May 1, 2012). "Expectations of privacy in the contents of a computer are likened to expectations of privacy in other types of containers, such as suitcases or briefcases. . . . 'Because intimate information is commonly stored on computers, it seems natural that [personal] computers should fall into the same category as suitcases, footlockers, or other personal items that command a high degree of privacy.'" *United States v. Trejo*, 2010 WL 940036 at *4 (E.D.Mich. March 12, 2010), *aff'd* 471 Fed. Appx. 442 (6th Cir. 2012), *quoting United States v. v. Andrus*, 483 F.3d 711, 718 (10th Cir. 2007). "Whether a defendant has a reasonable expectation of privacy in a particular place is a two-pronged inquiry. [The Court] consider[s] first, whether the movant has exhibited an actual, subjective, expectation of privacy; and second, whether such subjective expectation is one that society is prepared to recognize as objectively reasonable." *United States v. Werra*, 638 F.3d 326, 331 (1st Cir. 2011). Both of these requirements are amply satisfied here.

The netbook and hard drive belonged to Swartz, and he took pains to place the netbook and hard drive in locations in which they would be free from interference by outsiders, first in a basement data room which appeared from the outside to be locked, concealed under a box, Timeline at 6; Murphy Grand Jury at 82-83, and then under a table in a private area of the Student Center. Critically, the computer was password protected to prevent access to its contents. *See, e.g., United States v. Reeves*, 2012 WL 1806164 at *8 (May 17, 2012)(fact that defendant's computer was password protected was "sufficient to show her intent to exclude members of the public and maintain

privacy in the documents kept on her computer"); *Clements-Jeffrey v. City of Springfield*, 2011 WL 3207363 at *3 (S.D. Ohio July 27, 2011)("Personal computers that are password protected are subject to even greater privacy protection"); *United States v. Griswold*, 2011 WL 7473466 at *12 (W.D.N.Y. June 2, 2011)("In this age of electronically stored information a reasonably well trained police officer should know that an individual's use of a password to protect against unauthorized access to electronic files stored on his or her computer is no less an indication of personal privacy than the use of a lock and key by the owner of a file cabinet"); *Howe*, 2011 WL 2160472 at *7 (defendant's use of a password to protect the files on the computer demonstrates his subjective expectation of privacy in the contents); *see also Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001)(co-user of computer could not validly consent to search of defendant's password-protected files on the computer to which co-user did not have access). Swartz plainly had a subjective expectation of privacy in the netbook and the external hard drive.

That expectation, moreover, is one which society should recognize as objectively reasonable. The netbook was connected to the MIT network, but "the mere act of accessing a network does not in itself extinguish privacy expectations." *United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007). MIT has a liberal guest access policy, which was described by Tim McGovern, MIT Manager of Network Security & Support Services, as follows:

> No authentication of visitors. Visitor network access is provided as an on-demand self-service process for anyone who walks onto campus, plugs in, or elects to use our wireless network, and declares themselves a visitor, and they get 14 days of network privileges.
> No identity verification. Visitors are asked to provide an email address. The email address is not used to verify that a bona fide identity exists . . . .
> No authentication of users accessing JSTOR.org. By agreement, JSTOR.org allows any computer with a net 18 IP address [an MIT IP address] to access their resources without further identification or authentication.

Exhibit 3. Nothing on the MIT website relating to guest use of the MIT network diminishes this legitimate expectation of privacy. Nothing on the MIT website precludes guests – or students or

faculty members – from leaving their laptops in private areas of the campus while downloading data from the internet.

Contrary to the government's argument in its Response to Defendant Aaron Swartz's Motion for Discovery (Doc. 41) at 6, Swartz did not forfeit his expectation of privacy in his netbook and external hard drive because he was a trespasser; those items remained closed containers which were his personal property and which were not abandoned, *see* pages 11-12, *infra.* Swartz was not a trespasser at MIT in any sense. The MIT campus is not closed to persons other than students, faculty, and employees. On the contrary: it is an open campus with practices that encourage persons who are members of the broader Cambridge technical community to share its resources. Swartz has lectured to an MIT class, audited classes at MIT, worked on projects with MIT professors, and has been a valued member of MIT forums and groups.

The cases on which the government relied are uniformly inapposite. In *United States v. Terry*, 2007 WL 496630 (S.D.Ga. Feb. 12, 2007), *aff'd* 258 Fed. Appx. 304 (11th Cir. 2007), the defendant appropriated to himself a unit in a storage facility which he did not rent and had no right to occupy and affixed a padlock to it. Similarly, in *United States v. Pitt*, 717 F.2d 1334 (11th Cir. 1983), the defendant padlocked a room belonging to his girlfriend's landlady, to which his girlfriend, as the tenant, had no right of access or use, and which the landlady had reserved to her exclusive use. In *United States v. Hightower*, 1987 WL 44897 (6th Cir. Sept. 28, 1987), the defendant placed locks on country club lockers which he was not authorized to use and for which he had not paid the required fee. In *United States v. Sanchez*, 635 F.2d 47 (2d Cir. 1980), the defendant was unable to demonstrate ownership of or authority from the owner to possess and use the automobile which was the subject of the challenged search. What *Sanchez* says is that "a mere trespasser has no Fourth Amendment protection *in premises* he occupies wrongfully." *Id.* at 64 (emphasis added). Like the

other cases on which the government relied, *Sanchez* involved an assertion of a reasonable expectation of privacy in the entire premises at issue – the storage unit, the landlady's storage room, the car, the lockers – which is not the issue here. Swartz does not suggest that he had a reasonable expectation of privacy in the data room, but solely in his private property located therein – the netbook and the external hard drive – and in the electronic communications to and from his netbook. The data room was located within a network of hallways which were used by people to travel between MIT buildings, especially in the winter. Murphy Grand Jury at 82-83. There were classrooms on the same floor, and students used the corridor to attend classes. There were no signs ordering people to keep out, *see* Exhibit 27, and the door to the data room opened readily with a "quick jerk." Murphy Grand Jury at 84. Swartz simply was not a trespasser in the sense which led to the decisions in *Sanchez* and the government's other cases. *See United States v. Scott*, 673 F.Supp.2d 331, 339 (M.D.Pa. 2009)(defendant had reasonable expectation of privacy in computer belonging to him seized from apartment where defendant did not contend that he lived or stayed for any period of time or that he was ever invited to the apartment or that he had a key to the apartment).

Nor did Swartz abandon the netbook. To find abandonment, there must be "clear and unequivocal evidence" that the defendant intended to abandon the property. *United States v. Crist*, 627 F.Supp.2d 575, 580-81 (M.D.Pa. 2008)(holding that defendant did not abandon computer where he returned to house to get it 26 days after his rent became overdue, eviction proceedings had not commenced, and defendant had received no notice that his property would be removed), *quoting United States v. v. Fulani*, 368 F.3d 351, 354 (3d Cir. 2008). Here, Swartz neither denied ownership of the netbook nor physically relinquished the item. *See United States v. James*, 353 F.3d 606, 615-16 (8th Cir. 2003)(defendant did not abandon computer disks he gave to a friend to store, even after he told the friend to destroy them); *United States v. Upham*, 168 F.3d 532, 357 (1st Cir.

1999)(defendant did not abandon computer images by deleting them); *United States v. Infante-Ruiz*, 13 F.3d 498, 501-02 (1st Cir. 1994)(defendant did not repudiate privacy interests by leaving his unlocked briefcase in the locked truck of another person's car, even though he allowed other people to store items in it because "he did nothing to indicate its availability to the public generally nor did his actions betray an intention to forego an owner's normal right to exclude those he wished to exclude"). Notably, the law enforcement officials on the scene did not believe that the netbook was abandoned, as they set up video surveillance in anticipation of the owner's return, and, indeed, Swartz was observed returning to the netbook on the afternoon of January 4, 2011, and on January 6, 2011.

The netbook and external hard drive were seized from the Student Information Processing Board Office, a small private office located in the MIT student center, *i.e.*, it was not seized from the Building 16 data closet. A student who was present when Swartz entered the room, and whose identity is known to the government, told Cambridge Police that Swartz asked permission to use a network drop in the room, and the student pointed him to one. After the student told Swartz that he was leaving and needed to lock the room, Swartz left, as did the student, locking the door behind him. Thus, Swartz had the permission of a person with authority over the room (as evidenced by his possession of keys to it) to connect to the MIT network in the room and had every reason to believe that the netbook was in a private, locked space where it would remain unmolested. He had both a subjective and objectively reasonable expectation of privacy in the netbook and hard drive.

III. THE SEARCHES AT ISSUE HERE.

A. The January 4, 2011, and January 6, 2011, External Examination and Fingerprinting of the Netbook and Hard Drive.

While the netbook and external hard drive were in plain view, and law enforcement officers were lawfully on the premises, the physical manipulation of the netbook and external

hard drive by law enforcement personnel to examine its external attributes and to fingerprint it constituted a warrantless search within the meaning of the Fourth Amendment. *See, e.g., Arizona v. Hicks*, 480 U.S. 321, 324-25 (1987)(officer's moving of turntable to examine its exterior constituted Fourth Amendment search). As the Supreme Court explained in *Hicks*: "[T]he distinction between 'looking' at a suspicious object in plain view and 'moving' it even a few inches is much more than trivial for purposes of the Fourth Amendment. It matters not that the search uncovered nothing of any great personal value to respondent – serial numbers rather than (what might conceivably have been hidden behind or under the equipment) letters or photographs. A search is a search, even if it happens to disclose nothing but the bottom of a turntable." *Id.* at 325. *See, e.g., United States v. Paneto*, 661 F.3d 709, 714 n.3 (1st Cir. 2011)("Under *Hicks,* it is clear that the Fourth Amendment forbids handling an item to expose something hidden"). The same reasoning applies with equal force to the opening of the hard drive case and the examination of the hard drive contained within it. The fruits of the external examination of the netbook and the external hard drive and its case must, accordingly be suppressed.

B. The Internal Examination of the Netbook.

The opening of the netbook, the observation of the screen showing the operating system in use and the log-in screen, the attempts to bypass the log-in screen, and the conducting of an NMap search of the netbook to determine which ports were open, constituted a search within the meaning of the Fourth Amendment. *See, e.g., United States v. Musgrove*, 845 F.Supp.2d 932, 949 (E.D.Wis. 2011)(touching key or moving mouse to expose screen that was not previously in view is Fourth Amendment search); *United States v. Crist*, 627 F.Supp.2d 575, 585 (M.D.Pa. 2008)(running of hash values is a Fourth Amendment search); *see also United States v. Phillips*, 477 F.3d 215, 217 (5th Cir. 2007)(describing port scanning as "the

electronic equivalent of 'rattling doorknobs' to see if easy access can be gained to a room"). The internal examination of the laptop and its functions was a search, just as opening a locked briefcase or file cabinet and examining its contents is, and could not lawfully be conducted in the absence of a search warrant duly issued upon a showing of probable cause. The fruits of this internal examination must, accordingly, be suppressed.

C. The Capture of Electronic Communications to the Netbook.

18 U.S.C. §2510(12) defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce . . . ." Section 2510(4) defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." "Contents" is in turn defined as "any information concerning the substance, purport or meaning" of the communication. §2510(8). The "packet capture" which MIT continued to undertake at the recommendation of S/A Pickett and the persuasion of Det. Murphy captured the entire communication, including subject matter and content. That it intercepted the content of electronic communications is obvious from Newman's January 5, 2011, email to S/A Pickett informing him that he had "collected about 70G of network traffic so far with about 98% of which is the JSTOR journal downloads." Email chain at 2. Even accepting Newman's calculations, that means that 2% of the 70G of intercepted data, communications, emails, and the like, involved parties other than JSTOR, *see, e.g.,* Exhibit 28 (showing interception of communications of third party), a significant violation of the Fourth Amendment, as was the warrantless seizure of the 98% of the content emanating, according to Newman, from JSTOR. Obviously, Newman, working in concert with S/A

Pickett, must have searched his copy of the intercepted communications to make his numerical assessment. Use of the packet capture constituted the interception of electronic communications within the meaning of Title III, *see, e.g., United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005)(*en banc*)(diverting incoming communications constitutes interception within the meaning of Title III), which was unlawful in the absence of a valid order authorizing the interceptions of the electronic communications, of which none were sought or issued here.

None of the exceptions to the prohibition of warrantless interception of electronic communications are applicable here. Section 2511(2)(a)(i) provides:

> It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights and property of the provider of that service . . . .

This section is inapplicable here because, as more fully addressed in the next section of the memorandum, MIT personnel were acting as government agents beginning no later than 11:00 am on January 4, 2011, and the packet capture was conducted by them as government agents. Because they were acting as government agents, "the requirements of the Fourth Amendment . . . override statutory authority." *United States v. Pervaz*, 118 F.3d 1, 5 (1st Cir. 1997). *See McClelland v. McGrath*, 31 F.Supp.2d 616, 618 (N.D. Ill. 1998)("What the officers do not seem to understand . . . is that *they* are not free to ask or direct Cellular One to intercept *any* phone calls or disclose their contents, at least not without complying with the judicial authorization provisions of the Wiretap Act, *regardless* of whether Cellular One would have been entitled to intercept those calls on its own initiative" (emphasis in original)); *United States v. Auler*, 539 F.2d 642, 647 (7th Cir. 1976)("Government agents must not rely on telephone company employees to act on their behalf

without complying with the requirements of the Fourth Amendment. . . . In no situation may the Government direct the telephone company to intercept wire communications in order to circumvent the warrant requirements of a reasonable search"); *United States v. Hudson*, 2011 WL 4727811 at *3 (E.D.La. Oct. 5, 2011)("If the Alltel employees were government agents, . . . they would not satisfy the carrier exception of Title III, and their conduct would be judged under the standards of the Fourth Amendment").[8]

This conclusion is reflected in the USDOJ manual, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, which instructs that the provider exception "does not permit law enforcement officers to direct or ask system administrators to monitor for law enforcement purposes." *Id.* at 174-75. The Manual continues:

> After law enforcement and the provider have communicated with each other, . . . the cautious approach is only to accept the fruits of a provider's monitoring if certain criteria have been met that indicate that the provider is monitoring and disclosing to protect its rights or property. These criteria are: . . .(3) *law enforcement has not tasked, directed, requested or coached the monitoring for law enforcement purposes*, and (4) law enforcement does not participate in or control the actual monitoring that occurs.

Id. at 175 (emphasis added). Here, law enforcement plainly, at a minimum, "requested or coached the monitoring for law enforcement purposes." *See* Murphy Grand Jury at 66 (Murphy testified that after learning that MIT had begun the packet capture, "we" told MIT personnel that "[w]e'd like you to keep this running" and, ultimately, "we end up *persuading* them to leave that on the system"(emphasis added)). The provider exception is, accordingly, inapplicable.[9]

---

[8] MIT's interceptions prior to January 4, 2011, are addressed in a separate motion to suppress. *See* Motion to Suppress All Fruits of Interceptions and Disclosures of Electronic Communications and Other Information by MIT Personnel in Violation of the Fourth Amendment and the Stored Communications Act and Incorporated Memorandum of Law.

[9] Moreover, §2511(2)(a)(i) has a reasonableness requirement – an electronic communications service provider may intercept communications only insofar as such interception is "a necessary incident" to the protection of its rights and property. *See, e.g., United States v. Harvey*, 540 F.2d

The "trespasser" provision is also inapplicable. Section 2511(2)(i) provides:

> It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if –
>
> (I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;
>
> (II) the person acting under color of law is lawfully engaged in an investigation;
>
> (III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and
>
> (IV) such interception does not acquire communications other than those transmitted to and from the computer trespasser.

Section 2510(21) defines "computer trespasser" as "a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer." This provision is inapplicable for three separate reasons. First, Swartz was not a "computer trespasser" within the meaning of Title III because he did not "access a protected computer without authorization." Quite the contrary – he was validly signed on to the MIT network as a guest, as the MIT guest policy permitted him to be, and, accordingly, maintained a reasonable expectation of privacy in the communications to and from his netbook. That MIT regarded him as a guest user is confirmed by a number of MIT communications during the fall of 2010. On October 14, 2010, Ellen Duranceau, MIT Program Manager of Scholarly Publishing and Licensing, emailed Brian Larsen at JSTOR, informing him that "[o]ur investigations here point to the same *guest* that was involved in the 9/27 incident. We don't have enough

---

1345, 1351 (8th Cir. 1976); *United States v. Hudson*, 2011 WL 4727811 at *7 -*8 (E.D.La. Oct. 5, 2011). The packet capture went far beyond anything was necessary to the protection of MIT's rights and property. Once the netbook was identified, running, with an external hard drive, it was fully expected that the owner would return, hence the installation of video surveillance to identify the owner. The data capture was not relevant to protecting MIT's property as an electronic communication system provider.

information to follow the trail completely, but the signs suggest that the same *guest user* was responsible for this latest activity. . . . all of this excessive use was caused by a *guest visitor* at MIT" Exhibit 5 (emphasis added). JSTOR is available to "[u]sers [who] come to MIT to establish a guest account on the network, and "do not have to have MIT affiliation to use the content." Summary of Key Points by Ellen Duranceau, Exhibit 8. *See* Email from Ellen Duranceau to Ann Wolpert, October 15, 2010, Exhibit 9 ("we cannot identify the *guest* involved in these incidents" (emphasis added)); Email from Ellen Duranceau to Brian Larsen, October 15, 2010, Exhibit 10 ("[o]ur records and logs . . . do not allow us to definitively identify the *guest*" (emphasis added); Email from Ellen Duranceau to Tim McGovern, October 18, 2010, Exhibit 6 (asking if it would be accurate to say: "We offer guests access to the MIT network, and this practice will continue. However, once we institute our additional authorization layer for JSTOR, this route will be closed to guests"); Email from Ellen Duranceau to Rich Wenger, October 18, 2010, Exhibit 11 ("it appears that the individual used MIT's wireless network guest account process"). Second, the *content* of the communications was not relevant to the investigation. Third, just as the provider exception cannot override the protections of the Fourth Amendment, nether may the statutory trespasser exception. The Fourth Amendment is fully applicable to these interceptions.

IV. TO THE EXTENT THAT ANY OF THE SEARCHES AT ISSUE HEREIN WERE PERFORMED BY MIT PERSONNEL RATHER THAN LAW ENFORCEMENT OFFICERS, THE MIT PERSONNEL WERE ACTING AS AGENTS OF THE GOVERNMENT, AND THE FOURTH AMENDMENT IS FULLY APPLICABLE TO THEIR ACTIONS.

While purely private action is not subject to Fourth Amendment scrutiny, from the point that S/A Pickett and Det. Murphy arrived on the scene, the MIT personnel ceased to be private actors and, instead, acted to further the law enforcement investigation rather than the protection of MIT's interests. The First Circuit has identified three factors relevant to the determination whether a private individual was acting as a government agent: "the government's role in instigating or participating

in the search, its intent and the degree of control it exercises over the search and the private party, and the extent to which the private party aims primarily to help the government or to serve its own interests." *United States v. Pervaz*, 118 F.3d 1, 6 (1st Cir. 1997). *See, e.g., United States v. Hardin*, 539 F.3d 404, 419 (6th Cir. 2008)("the police must have instigated, encouraged or participated in the search," and "the individual must have engaged in the search with the intent of assisting the police in their investigative efforts"); *United States v. Souza*, 223 F.3d 1197, 1201-02 (10th Cir. 2000)(Police must "instigate, orchestrate, encourage or exceed the scope of the private search to trigger the application of the Fourth Amendment"); *United States v. Reed*, 15 F.3d 928, 931 (9th Cir. 1994)(inquiry is "(1) whether the government knew of and acquiesced in the intrusive conduct; and (2) whether the party performing the search intended to assist law enforcement efforts or further his own ends"); *see also United States v. Van Dyke*, 2010 WL 1949640 at *3 (W.D.Mich, May 14, 2010)("permitting the government to circumvent the limits of the Fourth Amendment by directing individuals to conduct searches that the government cannot, would totally undermine the purposes of the Fourth Amendment").

This standard is plainly met in this case, particularly with respect to the continuing packet capture of electronic communications to Swartz's netbook and the real-time provision of DHCP log information from January 4, 2011, through January 6, 2011.[10] Once S/A Pickett and Det. Murphy arrived on the scene, it became a law enforcement investigation. Once the netbook was located, no further investigation was necessary to protect MIT's rights or property. The investigation which began with the arrival of S/A Pickett and Det. Murphy was a law enforcement investigation with the object of identifying, arresting, and prosecuting the individual responsible for the downloads from

[10] *See* Motion to Suppress All Fruits of Interceptions and Disclosures of Electronic Communications and Other Information by MIT Personnel in Violation of the Fourth Amendment and the Stored Communications Act and Incorporated Memorandum of Law.

JSTOR. The netbook was left in place, with MIT continuing to monitor it at the recommendation of S/A Pickett and upon the urging of Det. Murphy. *See* page 3, *supra.* The monitoring strategy was developed in consultation with S/A Pickett and Det. Murphy. The monitoring was continued because law enforcement wanted to gather evidence of intent and motive, *see* page 6, *supra*, matters of no relevance whatsoever to the protection of MIT's interests. MIT recognized on January 4, 2011, that "[t]he investigation ha[d] moved beyond MIT was [was] now being handled by law enforcement." Exhibit 22. MIT personnel asked S/A Pickett on January 5, 2011, "what the next step [was]," Exhibit 25, further illustrating S/A Pickett's direction of the investigation. Halsall admitted that he was "gathering up all the stuff for Pickett." Exhibit 26. MIT personnel asked S/A Pickett's permission before taking the netbook offline and asked him whether they should image the netbook. *See* page 6, *supra.* In an email from Halsall to S/A Picket on January 8, 2011, Halsall told Pickett that he "hop[ed] to have the pcap/flows/videos/logs all in by to me Monday, possibly sooner – if you don't already have a copy of the video or pcap [packet capture], I'll make sure you get one." Exhibit 2.

Here, the government plainly encouraged the search, played a role in its design and operation, and MIT personnel deferred to the guidance of law enforcement officers, aiming to assist the government in its criminal investigation rather than being motivated by its own interests. Beginning with the arrival of S/A Pickett and Det. Murphy on January 4, 2011, MIT personnel were acting as government agents, and the requirements of the Fourth Amendment are fully applicable to any search or interception of electronic communications conducted by them. These interceptions were unlawful in the absence of a warrant, issued upon a showing of probable cause. The intercepted communications, as well as all derivative fruits thereof, must be suppressed.

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 5th day of October, 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. One copy of the exhibits to the motion was served on the government by hand this same date.

/s/ Martin G. Weinberg

Martin G. Weinberg