UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA, v. AARON SWARTZ, Defendant.	No. 11-CR-10260-NMG PUBLIC VERSION

DEFENDANT'S REPLY IN SUPPORT OF MOTIONS TO SUPPRESS AND MOTION TO DISMISS COUNTS 1 AND 2 OF SUPERSEDING INDICTMENT

(Leave to File Granted by Electronic Order dated November 13, 2012)

Aaron Swartz has moved to suppress five categories of evidence illegally obtained by the Government, including: (1) the "packet capture" of communications made by Swartz's ACER laptop while it was connected to the MIT network; (2) logs of network activity provided by MIT to law enforcement; (3) the fruits of the search of the exterior and interior of the ACER laptop while it was connected to the MIT network; and (4) the fruits of the search of the ACER laptop, Western Digital hard drive, and HP USB drive carried out pursuant to warrants first sought thirty-four days after the equipment was seized. Dkts. 59-63.[1] Also pending before the Court is Swartz's motion to dismiss Counts 1 and 2 of the Superseding Indictment. Dkt. 64. The Court should grant all these motions for the reasons laid out in the motions and this Reply.

Moreover, the Government's opposition briefs, Dkts. 81-82, make clear that many facts crucial to resolution of the pending motions remain in dispute. To resolve those disputes and decide the motions, the Court must hear testimony and receive evidence from witnesses with MIT, JSTOR, and the law enforcement agencies involved in the underlying investigation. Accordingly, Swartz respectfully asks the Court to hold an evidentiary hearing prior to deciding

[1] As to a fifth category of illegally obtained evidence, the Government has stated that it does not intend to offer either the network scan of the ACER laptop's ports or evidence derived from searches of Swartz's apartment and office during its case in chief. *See* Dkt. 81 at 34-35 n.23, 45. As a result, this Reply does not discuss the reasons why that evidence ought to be suppressed. Swartz maintains the objections to that evidence noted in his motion to suppress and reserves his right to challenge that evidence in the event the Government elects to offer it before or at trial.

the pending motions.

I. THE EVIDENCE OBTAINED AS A RESULT OF THE WARRANTLESS SEARCHES MUST BE SUPPRESSED

A. Swartz had a reasonable expectation of privacy in his laptop computer and its electronic communications

The Government contends Swartz had no reasonable expectation of privacy in his ACER laptop computer, its contents, and its electronic communications. But whether Swartz had a reasonable expectation of privacy can be evaluated only in the specific factual context of this case. It requires an analysis of MIT's specific policies and practices regarding computer use and privacy on the MIT campus, a community uniquely saturated with electronic devices. But as of now, there is nothing in the record before the Court describing this relevant context. The only reliable way to establish that context, and evaluate the reasonableness of Swartz's expectations, is for the Court to hear testimony from MIT officials and community members at an evidentiary hearing prior to the resolution of these motions.

Swartz believes such testimony will demonstrate he had both a subjective and objectively reasonable expectation of privacy in the ACER laptop and its contents when he placed the laptop in quiet and infrequently accessed locations—Room 16-004t in Building 16 ("Room 004") and the locked office in the student center—where it was unlikely to be disturbed or stolen. Given MIT's open campus, virtually any room of which can be accessed by anyone walking off the street, Swartz specifically chose to place his computer somewhere where it would not be stolen, as it might be if he left it in a classroom or on a desk at the library. He sought and received permission from a student monitor to leave his computer in the locked office in the student center and, as further discussed in section I.B below, did not wrongfully enter Room 004. Swartz also returned to Room 004 twice over the course of three days to check on his property and password-protected his computer to provide an additional level of security. *See, e.g., United States v. Reeves*, 2012 WL 1806164, at *8 (D.N.J. May 17, 2012) (password-protection was sufficient to show intent to maintain privacy in documents kept on computer).

It was also objectively reasonable for Swartz to expect that MIT would not violate (as it did) its obligations under the Stored Communications Act, the Wiretap Act, and the Massachusetts Wiretap Act by disclosing the electronic communications between his computer

and the MIT network at the direction of government agents. With respect to information in the MIT DHCP server logs, the objective reasonableness of Swartz's privacy expectation is further bolstered by MIT's own official policy, which specifies that DHCP logs will only be disclosed under the direction and approval of MIT's Office of the General Counsel—which presumably would ensure that MIT would not violate any electronic privacy laws. *See* IS&T Policies: DHCP Usage Logs Policy, https://ist.mit.edu/about/policies/dhcp-usage-logs (last visited Nov. 28, 2012). Even if Swartz's experience with software engineering made him aware that MIT might ***monitor*** his IP and MAC addresses during the time he was logged onto the network, there is no evidence that he knew or suspected that MIT would permanently record such information, much less share it with outsiders in violation of various applicable laws. *See* http://ist.mit.edu/about/policies/dhcp-usage-logs (last visited Nov. 30, 2012) (stating that MIT retains DHCP logs for only 30 days after creation); *see also United States v. Heckenkamp*, 482 F.3d 1142, 1146 (9th Cir. 2007) (holding that the mere act of accessing a network does not extinguish privacy expectations). Consequently, Swartz had a reasonable expectation that MIT would not work hand-in-hand with law enforcement to illegally intercept, capture, and disclose his electronic communications while he was connected to MIT's open network as an authorized guest.

B. The packet capture of the laptop computer cannot be justified under the trespasser exception to the warrant requirement

The Government concedes that the January 4, 2011, packet capture of the ACER laptop's communications involved interception of the contents of those communications under color of law, and thus required a Title III order that the Secret Service failed to secure. Nonetheless, the Government attempts to salvage its warrantless seizure of the packet capture by arguing that Swartz "was a trespasser on MIT's system." Dkt. 81 at 23-25. The Government is wrong on the facts. All the purportedly undisputed "facts" asserted by the Government in support of its trespasser argument are either provably false or hotly disputed, which is yet another reason for the Court to hold an evidentiary hearing before deciding the pending motions.

The Government begins by erroneously claiming that Swartz physically trespassed onto MIT's campus, supporting this assertion by appending a single photograph of a single door somewhere on the MIT campus that happens to have a "no trespassing" sign. *See* Dkt. 81-8.

Apart from the fact that this image is undated and unauthenticated,[2] the Government neglects to mention that, in addition to this one door, there are myriad ways for anyone to gain access to Building 16's basement, including many that do not require entrance from the street. All of MIT's main buildings, including Building 16, are freely accessible through an extensive network of tunnels and hallways. More importantly, the Government does not dispute that MIT maintains an open campus. MIT affirmatively invites the public to visit its campus, tour its buildings, and attend lectures and events throughout the year, and so merely entering campus public spaces cannot be considered a trespass. *See* http://mitadmissions.org/visit/visit (last visited Nov. 26, 2012) ("The MIT campus is open to the public year-round."); http://web.mit.edu/institute-events/visitor/ (last visited Nov. 26, 2012);[redacted] Neither Building 16 nor its basement was locked; both were readily accessible by any member of the public.[3]

Moreover, the Government's claim that Swartz accessed Room 004 by opening "locked steel doors" is fictional. Contemporaneous video surveillance taken from inside the room contradicts this characterization. That footage reveals that the doors to the room were often left ajar, and were accessed by numerous individuals at different times, none of whom needed or used a key to do so. [redacted] Room 004 itself was clearly accessible to the public, as evidenced by the large amount of graffiti on its walls, *see* Dkt. 81-10, and surveillance footage of unidentified individuals accessing the room or using it to store garbage bags.

Finally, the Government incorrectly asserts that Swartz "trespassed" on MIT's network. But MIT's network was open to anyone present on its campus, regardless of whether they had any affiliation with MIT or other formal reason to be there. *See* Dkt. 68, Ex. 3 (stating that visitor access is provided on-demand to anyone who walks onto campus)[redacted] Further, access to the network did not require any user identification,

[2] The Government has not authenticated any of the images and screen shots cited as exhibits in its opposition with an accompanying declaration. Many of the images and screen shots lack any information identifying the date they were taken. To the extent the Government wants to rely on these images to defeat suppression, it must lay some foundation permitting the Court to believe they are what the Government asserts they are.

[3] In addition, Swartz was not a mere visitor to MIT; he was an established member of the MIT community who had given a guest lecture, audited MIT classes, worked on projects with MIT professors, and attended events on campus on multiple occasions.

password, or other verification. While the Government points to Defendant's use of pseudonyms when registering for network access, that makes no difference for purposes of access. MIT never took any steps to actually verify the identity of network users prior to granting access or restrict use by people entering pseudonyms when they logged on. *See* Dkt. 68, Ex. 3. Swartz was not a trespasser at MIT and is entitled to the full protections of the Fourth Amendment.

C. The Government has failed to excuse law enforcement's decision to conduct warrantless searches of the computer's interior

The Government throws out a variety of explanations for the investigators' failure to seek a warrant to open up and search Defendant's computer in hopes that one will stick. But neither the plain view doctrine nor MIT's consent to search Room 004 justify law enforcement's decision to open and inspect the computer while it was in the room, rather than disconnecting it from the network and seizing it for a later search pursuant to a warrant. The Government's argument that the search was constitutionally valid because Swartz's computer was "wrongfully" present in Room 004 is unavailing, for the same reasons Swartz was not a trespasser.

The Government also argues that the investigators' decision to open the computer was justified by "exigent circumstances," because a computer's random access memory ("RAM") information is lost when the computer is turned off. *See* Dkt. 81 at 35-36. But there was no exigency here. Investigators could have seized the computer, disconnected it from the network, and obtained a warrant to search its RAM prior to powering the computer down. There was no imminent risk that the computer would spontaneously shut down during the time that it was within law enforcement's control. Instead, the Government created its own "exigent circumstances" by choosing to leave the computer connected to the network and inside Room 004 in an attempt to lure the computer's owner into revealing himself, seeking an investigatory benefit in exchange for the risk that the owner would turn the computer off. Accordingly, the Government cannot justify the search of the computer's interior without a warrant and the fruits of that search must be suppressed.

II. THE DELAY IN OBTAINING WARRANTS TO SEARCH DEFENDANT'S COMPUTER EQUIPMENT VIOLATED THE FOURTH AMENDMENT

The Secret Service's ***34-day delay*** in obtaining search warrants for (1) the ACER laptop; (2) the Western Digital hard drive; and (3) the HP USB drive rendered seizure of those items

unreasonable under the Fourth Amendment. Accordingly, the Court must suppress the fruits of the searches eventually conducted on those items.

The Government attempts to avoid the consequences of its unreasonable delay with four specious arguments. *First,* it argues the Cambridge Police were entitled to hold the laptop, hard drive, and USB drive for an unlimited period of time as physical evidence of computer crimes, larceny, and breaking and entering, analogizing the seized items to "a bag of burglar tools." Dkt. 81 at 47. But this same argument was recently rejected, and rightly, in *United States v. Shaw*, 2012 WL 844075, at *3 (N.D. Ga. Feb. 10, 2012), which held that cell phones seized during an arrest were not evidence of a crime in and of themselves, because phones are not contraband and do not have evidentiary value apart from their contents.

Just as was true for the phones in *Shaw*, Swartz's computer hardware is not contraband in and of itself. Unlike a burglar's bag of tools, computers have a multitude of legitimate uses and play a routine and increasingly essential role in everyone's daily life. *See United States v. Mitchell*, 565 F.3d 1347, 1351 (11th Cir. 2009) (observing that there is a strong possessory interest in computer hard drives because they are heavily relied upon for personal and business use). Moreover, the Government has not explained with any level of specificity ***how*** the computer hardware, as distinguished from its contents, offers any physical evidence of the charged crimes. *See Shaw*, 2012 WL 844075 at *3; *see also United States v. Wright,* 2010 WL 841307, at *10 (E.D. Tenn. Mar. 3, 2010) ("Ordinarily, of course, a suspect's possession of a computer will have no evidentiary value apart from its contents.").[4]

Second, the Government claims that the Secret Service's unexplained delay cannot have harmed Swartz's possessory interests in the computer media because he never asked the investigators for his equipment back. This makes no difference. A defendant's Fourth Amendment rights do not depend and never have depended on whether he expressly seeks the

[4] Even if the Government had offered a specific reason that the laptop and hard drive amounted to physical evidence of a crime, rather than being of evidentiary value for their contents alone, there is absolutely no connection between the alleged Massachusetts crimes and Swartz's possession of the HP USB drive at the time of his arrest. Possession of a USB drive while riding a bike on a public street is an entirely innocent activity and the investigators had no evidence that the USB drive was ever even present in Room 004. Accordingly, the drive's seizure cannot conceivably be justified based on an argument that it was physical evidence ***in and of itself*** of computer crimes, breaking and entering, or larceny.

return of wrongly seized property. Courts routinely suppress evidence seized after unreasonable delays in applying for search warrants, even where the defendant never demanded return of his belongings. *See Shaw*, 2012 WL 844075 at *3 (defendant's failure to request return of cell phones was immaterial to result); *see also United States v. Mitchell*, 565 F.3d 1347, 1348-53 (11th Cir. 2009); *United States v. Riccio*, 2011 WL 4434855, at *1-*3 (S.D. Cal. Sept. 23, 2011); *United States v. Rubinstein*, 2010 WL 2723186, at *12-*14 (S.D. Fla. June 24, 2010).[5] As Swartz pointed out in his motion, *see* Dkt. 63 at 4-5, courts have found delays much shorter than 34 days to be unreasonable and to require suppression. *See Mitchell,* 565 F.3d at 1350 (21-day delay in seeking search warrant was unreasonable).

Third, the Government remarkably suggests the Secret Service cannot be held responsible for its lackadaisical attitude toward seeking a search warrant because the Cambridge Police Department, not the Secret Service, was in possession of the computer equipment during the thirty-four day delay. It is telling that the Government fails to cite a single case in support of this proposition. Accepting this argument would allow one government agency to end-run Fourth Amendment requirements in the easiest manner imaginable—by leaving wrongly seized evidence in the possession of some other, closely cooperating government agency. Here, the Secret Service was plainly in charge of the investigation at MIT. It is absurd to suggest that it had no control over the seized computer equipment when its investigation directly resulted in that equipment being kept in the possession of the Cambridge Police. *See* Dkt. 68, Ex. 31 (report states that Secret Service Agent Pickett apprehended and handcuffed Swartz); Dkt. 68, Ex. 15 (report states that Pickett examined ACER laptop before turning it over in evidence bag to MIT Police). [redacted]

Finally, the Government asserts that the Secret Service's delay in seeking a warrant was

[5] In support of its contention that Swartz lacked a possessory interest in his computer equipment, the Government asserts that Swartz left his laptop unaccompanied for three months. This is speculation, as the Government has never pleaded any facts, as opposed to stating conclusions, indicating that Swartz's laptop was left unattended at any time prior to January 4, 2011.

justified because the computer crime at issue was "complex" and involved gathering "technical and specialized information." Dkt. 18 at 53-54. But the Government cannot simply assert this conclusion without proving it with evidence. In order to outweigh Swartz's strong possessory interest in his equipment, the Government must present a "compelling justification" for the delay in applying for a warrant. *Mitchell*, 565 F.3d at 1351; *see also Riccio*, 2011 WL 4434855 at *1 (faulting the government for not presenting any specific facts to explain need for delay). The Government offered no declaration from any of the officers involved in the pre-warrant investigation regarding technical complexity, nor pointed to even one piece of technical information presented in the warrants that necessitated over a month of delay between the seizure of the items and the application for a search warrant.

Moreover, the warrant applications specifically averred that Secret Service Agent Pickett was specially trained in the investigation of crimes involving unauthorized intrusions into computer networks. *See, e.g.*, Dkt. 68, Ex. 30. The Government has not indicated any unique circumstances that made this investigation particularly difficult for an agent with such extensive experience in the field of computer crimes. As it stands, the Government's response is simply a bare-bones conclusion that does not establish a "compelling justification" for the delay. At the very least, the Court should hear testimony from Agent Pickett regarding why the Secret Service delayed at such length before applying for a warrant.

III. THE WIRE FRAUD COUNTS MUST BE DISMISSED BECAUSE THE GOVERNMENT HAS FAILED TO ALLEGE A MISREPRESENTATION

The Court should also dismiss Counts 1 and 2 of the Superseding Indictment, because—as the Government's opposition makes clear—those wire-fraud counts are an improper attempt to apply an amorphous, overly broad federal statute that simply does not fit the charged conduct. The wire fraud charges cannot survive Defendant's motion to dismiss because, as the Government concedes, wire fraud requires a material misrepresentation. *See* Dkt. 82 at 2-3 (list of alleged misrepresentations); *see also Neder v. United States*, 527 U.S. 1, 16 (1999) (to be material, false statement must have natural tendency to influence, or be capable of influencing, decision of body to which it was addressed). The indictment does not sufficiently allege any such misrepresentation.

Nothing about Swartz's access to MIT's network, or to JSTOR through MIT's network, depended on or was influenced by any alleged misrepresentation. MIT's open network permits any person on MIT's premises free and full access, without requiring any user identification or password. At the time of the alleged offenses, MIT's network asked a user to enter a name and email address, but took no steps to verify that name or address, or to grant or deny access depending on the name or address entered. Dkt. 68, Ex. 3. An MIT guest would obtain the same full access to the MIT network whether she entered her real name or "Donald Duck" in the name field. Accordingly, Swartz's alleged use of pseudonyms cannot possibly have materially influenced MIT's decision to grant him access to the network. And, once Swartz was on the MIT network as an authorized guest user, he similarly gained full access to the JSTOR database under the terms of JSTOR's agreement with MIT. In fact, JSTOR's Terms and Conditions of Use specifically define "authorized users" under university contracts as including "on-site users physically present on the Institutional Licensee's premises." Dkt. 81-3. Consequently, Swartz was an authorized JSTOR user merely by virtue of his presence on MIT's campus.

Likewise, a computer's IP is not a constant, unalterable feature, like an automobile's VIN number. A computer is assigned an IP address each time that computer accesses a network, and this results in the same computer using a different IP address from day to day. Moreover, all major computer operating systems makes it trivially simple for any user to change the computer's IP address, which ability is useful for troubleshooting purposes when the computer is having difficulty communicating with a network. Until recently, computer users were frequently required to manually enter an IP address in order to connect the machine to the Internet. Neither is a MAC address a static feature of a device. Not only can a MAC address be changed with a few clicks of a mouse in every major operating system, the ability to change a MAC address is a required feature of personal computer hardware. Accordingly, neither an IP addresses nor a MAC address is necessarily associated with, or can be used as a reliable identifier for, any given user. A change to either does not represent any misrepresentation about a user's identity.

The Government also contends that Swartz violated JSTOR's terms of service by using a software program to create multiple JSTOR sessions and download a large volume of articles. In the first place, the Government offers no evidence that Swartz was ever presented with, much

less accepted, JSTOR's terms of service. [redacted] Finally, the Government has merely alleged that Swartz hid his computer in a basement room, not that he misrepresented its location to anyone. Because the Government has not alleged any affirmative misrepresentation by Swartz, it has not pleaded a wire fraud claim, and the Court should dismiss Counts 1 and 2.[6]

IV. CONCLUSION

For all the above reasons, the Court should either grant Swartz's motions to suppress and motion to dismiss or conduct an evidentiary hearing regarding those motions to resolve any factual disputes necessary to resolve those motions.

Respectfully submitted,

Dated: December 3, 2012 By: */s/ Elliot R. Peters*

Elliot R. Peters (*pro hac vice*)
Daniel Purcell (*pro hac vice*)
KEKER & VAN NEST LLP
633 Battery Street
San Francisco, CA 94111-1809
Telephone: 415 391 5400
Facsimile: 415 397 7188
epeters@kvn.com
dpurcell@kvn.com

Michael J. Pineault
Clements & Pineault, LLP
24 Federal Street
Boston, MA 02110
Telephone: 857 445 0135
Facsimile: 857 366 5404
mpineault@clementspineault.com

Attorneys for Defendant AARON SWARTZ

[6] If the Court grants Swartz's motion to dismiss, the Government will remain free to pursue the ten separate counts in the Superseding Indictment alleging violations of 18 U.S.C. § 1030.

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, and paper copies will be sent on December 3, 2012 to those indicated as non-registered participants.

Dated: December 3, 2012

/s/ Elliot R. Peters
Elliot R. Peters