MEMORANDUM OF LAW

I. FACTUAL BACKGROUND.

On September 26, 2010, MIT received an email from (b)(6),(b)(7)(C) at JSTOR, an online archive of scholarly journal articles, informing it that there had been, that morning, an excessive downloading of journals. By the next day, the IP addresses from which the journals were being downloaded had been located (largely, if not exclusively, by JSTOR) and the user information for the guest registration of the computer being used had been identified; JSTOR then blocked access to these IP addresses. Timeline of events related to JSTOR downloading incident: 9/26/10 - 1/6/11, Exhibit 1 ("Timeline") at 1. On October 9, 2010, JSTOR again notified MIT that its access was being blocked because of excessive downloading. Timeline at 2. JSTOR quickly identified the IP address being used for the downloads, and MIT personnel thereafter discovered that access was being accomplished in Building 16 by a computer registered through its visitor guest registration process by the same guest whose computer was linked to the September incident.[3] Timeline at 2-3.

MIT and JSTOR conferred regarding methods to prevent excessive downloading. Timeline at 3-4. On December 26, 2010, there was another episode of excessive downloading, which MIT personnel did not learn of until on or about January 3, 2011. On the morning of January 4, 2011, at approximately 8:00 am, MIT personnel located the netbook being used for the downloads and decided to leave it in place and institute a packet capture of the network traffic to and from the netbook.[4] Timeline at 6. This was accomplished using the laptop of Dave Newman, MIT Senior

---

[3] MIT personnel first received notice of the October 9, 2010, incident when they returned following the Columbus Day holiday on October 12, 2010. Timeline at 2.

[4] A packet capture captures the entire communication, including subject matter and content, and to the extent it was diverting and copying communications in transit to and from the netbook, this constituted a classic interception of electronic communications in violation of *United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005)(*en banc*). *See* page 9, *infra*.

a password, a formal affiliation with the school, or any form of identification for any visitor to become an authorized guest enjoying access to the MIT electronic communication service which was the equal of that afforded to MIT students and professors.

Swartz was validly signed on to the MIT network as a guest, as the MIT guest policy permitted him to be, as verified by an October 14, 2010, email from Ellen Duranceau, MIT Program Manager of Scholarly Publishing and Licensing, to [redacted] 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 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), and then by an October 18, 2010, email from Ms. Duranceau to Tim McGovern, MIT Manager of Network Security & Support Services:

> Tim and Mike:
> Would it be accurate for me to answer [JSTOR's] query this way:
>
> "*We offer guests access to the MIT network, and this practice will continue.* However, once we [in the future] institute our additional authorization layer for JSTOR, *this route will be closed to guests.* So we will have closed the pathway used."
> * * * *
> Mike, I will be asking JSTOR about your mod_rewrite idea once I check in with Rich Wenger in the Libraries and once JSTOR has shifted more clearly into implementing the new method rather than still working on resolving the excessive use issue.

Exhibit 6 (emphasis added). Thus, MIT had an open-access network that permitted anyone to access it by signing in as a visitor/guest, and anyone signed in to the MIT network was permitted to access JSTOR without further identification or authorization. The name and email address used to sign in as a visitor were fundamentally irrelevant to MIT, as it did not use it in any way to identify the visitor or even to ascertain whether it was a "bona fide identity," nor did guests to the MIT network receive notice that they were prohibited from using static IP addresses, changing IP addresses, or changing MAC addresses when accessing the MIT network on successive occasions. Neither MIT nor JSTOR

initiated the additional authorization protocol prior to the seizure of the netbook and Swartz's arrest on January 6, 2011.

That MIT regarded Swartz as a guest user is also confirmed by several other MIT communications during the fall of 2010. On September 29, 2010, Ellen Duranceau informed (b)(6),(b)(7)(C) at JSTOR that "the origin of the activity was *a guest visiting MIT*." Exhibit 7 (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 (b)(6),(b)(7)(C), 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 Rich Wenger, October 18, 2010, Exhibit 11 ("it appears that the individual used MIT's wireless network guest account process").

In addition, MIT's written policy on DHCP logs created a reasonable expectation of privacy in *that* information, providing that they would be deleted after 30 days, IS&T Policies:DHCP Usage Logs Policy, available at http://ist.mit.edu/about/policies/dhcp-usage-logs (last visited September 24, 2012), and that they would be disclosed *only* in response to a court order or subpoena:

> When any network device, e.g., a computer, connects to MITnet and is assigned a dynamic IP address, MIT's DHCP server adds a record to its log containing the following information:
>
> - The date and time of the request
> - The MAC address of the requesting device or computer
> - The IP address provided
> - The specific DHCP command that was issued
> - Other technical information related to the request
>
> In the event of a request relating to a potential legal proceeding, IS&T staff may create a case in Request Tracker and store subsets of a log pertinent to the case at hand in the case record.

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 (b)(6),(b)(7)(C) 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.

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 (b)(6),(b)(7)(C) 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 (b)(6),(b)(7)(C), 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, neither 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

MIT Police, (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) for Network and Infrastructure Services for MIT, and (b)(6), in the basement of building 16. (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) from the Cambridge Police Department processed the scene for fingerprints. The netbook found connected to the switch in the wire closet in the basement of building 16 was an Acer Aspire One with a serial number LUSAK0D0010011100E1601. Network traffic indicated that the netbook was using two IP addresses (18.55.6.240 and 18.55.7.240) which are both IP addresses belonging to MIT. Use of NMap showed that the netbook had port 22 and 8092 open. Port 22 is the default port for SSH (Secure Shell network protocol) and port 8092 is often associated with TCP (Transmission Control Protocol) traffic. A surveillance camera was placed in the wire closet to record anyone returning for the netbook.

Continuing on 01/04/11, at approximately 1526, the surveillance camera recorded a white male, later identified as Aaron Swartz (DOB 11/08/86), enter the wire closet. Based on the surveillance video, Swartz appeared to replace the external hard drive with a new one and take the old hard drive with him.

Further on 01/04/11, (b)(6),(b)(7 was able to provide SA (b)(6),(b) with the following timeline regarding this investigation:

On 09/26/10, (b)(6),(b)(7)(C) the MIT (b)(6),(b)(7)(C) received an email from (b)(6),(b)(7)(C) the JSTOR (b)(6),(b)(7)(C) stating that excessive downloading of journals had been detected from MIT, and that all of MIT access to JSTOR would be blocked. JSTOR converts printed scholarly journals into electronic form and stores them in a central archive that can be accessed by libraries and institutions such as MIT.

On 09/27/10, the MIT Network and Information Security Team received an email from (b)(6),(b)(7)(C) the MIT (b)(6),(b)(7)(C) regarding excessive downloading from two IP addresses 18.55.6.216 and 18.55.6.218. JSTOR restored MIT access but blocked access to the identified IP addresses. (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) mit.edu), (b)(6),(b)(7)(C) (b)(6),(b)(7) discovered network registration for "Gary Host" with email address ghost@mailinator.com, a MAC address of 00235a735ffb and computer name "ghost-macbook" registered on the network on 09/24/10. (b)(6),(b) disabled the computer registration.

On 10/09/10, (b)(6),(b)(7)(C) from JSTOR Operations Staff, emailed (b)(6),(b)(7)(C) the MIT (b)(6),(b)(7)(C) to inform her that MIT's access to JSTOR had been cut off again due to excessive downloading.

On 10/12/10, the MIT Network and Information Security Team received an email from (b)(6),(b)(7)(C) stating that JSTOR informed her that excessive downloading came from IP address 18.55.5.100.

On 10/13/10, (b)(6),(b)(traced the second occurrence of excessive unauthorized downloading to a computer registered on the network as "Grace Host" with an email of ghost42@mailinator.com, a MAC address of 0017f22cb074 and computer name of "ghost-laptop". (b)(6),(b)(7 disabled the host registrations identified as bogus. (b)(6),(b)(7) (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) for MIT, notified that information indicated that the same unknown person appears to be using MIT guest registration from a wired connection in building 16.

On 11/29/10, the MIT Network and Information Security Team was notified by the MIT branch of the Institute of Electrical and Electronic Engineers that journal spidering has occurred on their site and it was tracked to the Student Information Processing Board XVM cluster, a group of computers that are shared and that anyone in the MIT community can use to host a Virtual Machine.