THE DECEMBER 2010 BLACK HOLE IN THE NETWORK INTERFACE CLOSET

As I've suggested, I'm very interested in pinpointing when and how the Federal government first got involved in the investigation of the JSTOR downloading and what role MIT had in the Feds getting involved. While Swartz' lawyers put together a timeline of the investigation, it constitutes grand jury material that is currently sealed (though you can be sure the content of it would have been aired during Swartz' trial).

And while we can get a pretty good idea of how the investigation proceeded from court documents, there two periods about which I have questions: December 2010, and the day of January 4, 2011.

The timeline below shows how Swartz allegedly accessed JSTOR documents, along with the response that JSTOR, MIT, and the government took. As you can see, the investigative narrative sort of fades out for the entire month of December 2010, when Swartz had a computer hooked right into MIT's network. And then—due to what gets vaguely described as new tools to track flows on MIT's own network—they found Swartz' computer. But there's a weird lapse in time, too: JSTOR notes that Swartz is downloading again around Christmas. But MIT

doesn't go find the computer—which it has recently acquired the ability to do—until January 4. Note, too, that the indictment treats the downloads from November 29 to December 26 as one charge, and those from December 27 to January 4, as another.

That leads to January 4, 2011, when according to the public fillings, the Cambridge cops and Secret Service got brought in and—almost immediately—SS takes over the case and MIT hands over data flow materials to SS without demanding a warrant. HuffPo explained that process this way:

> According to the source close to the investigation, when MIT employees found the laptop, they contacted MIT police, who called Cambridge police, where the call was then routed to a detective assigned to the New England Electronic Crimes Task Force. That detective contacted another member of the task force, Michael Pickett, a special agent with the U.S. Secret Service, who helped lead the investigation.

In addition, MIT allows SS to get Carnegie Mellon's CERT to collect the signals from Swartz' laptop in a dropbox; when Swartz' lawyers first asked for CERT's notes on that data flow, the government refused to turn it over, saying that since they would not call any CERT experts to testify they didn't have to.

I'm wondering several things. First, what were the new tools MIT used to analyze their networks in December 2010? Where did they come from? When did they get them? Was the JSTOR download the reason they did?

And also, what kind of legal analysis did MIT go through before they just let the government into their networks?

Finally, what obligations was MIT under to file Suspicious Activity Reports to the government regarding the JSTOR downloads and when did those

obligations kick in? Did MIT comply with those obligations? Did the government know MIT's network was compromised as early as September, or not until Cambridge brought in SS in January?

To be clear: I'm not suggesting anything nefarious about this—though I am mindful of this, from the scope of the investigation MIT President Rafael Reif has ordered: "I have asked that this analysis describe the options MIT had and the decisions MIT made, in order to understand and to learn from the actions MIT took." That is, Reif now wants to know which of the decisions MIT pursued they had legal choices to avoid.

The government's consolidated response to Swartz' suppression motion claims that "neither local nor federal law enforcement officers were investigating Swartz's downloading action before January 4, 2011, when MIT first found the laptop." Note, they refer just to Swartz' downloading action, not Swartz (though that may just be legal particularity), so it is possible though unlikely that federal law enforcement officers were investigating other activities of Swartz before then (we know the FBI had investigated his PACER downloads the previous year).

Note: the following timeline depends on the assertions of both the government and Swartz' lawyers. It represents alleged facts as presented by self-interested parties, not uncontested facts. Documents used include the hardware search warrant affidavit, superseding indictment, motion for discovery, pre January 4 suppression motion, January 4-6 suppression motion, consolidated response to motion to suppress, and exhibit to supplement to motion to suppress. I've also included Swartz' FOIAs, as described in this Jason Leopold story, because I find some of the coincidences intriguing (see especially the timing of his request for Secret Service access to encrypted files and CERT, which I'll return to in a later post).

September 25, 2010: Swartz logs into MIT's network (presumably via wifi) from Building 16.

September 25, 2010: JSTOR blocks access to Swartz' assigned IP address.

September 26, 2010: Swartz assigns himself a new IP address and resumes dowloading.

September 26, 2010: JSTOR blocks over 250 IP addresses.

September 27, 2010: MIT prohibits guest registration for any computer with Swartz' computer's MAC address.

October 2, 2010: Swartz spoofs his computer's MAC address, logging in with new IP address.

October 8, 2010: Swartz logs in second computer.

October 9-12, 2010: JSTOR blocks all of MIT's network access to JSTOR.

October 13, 2010: MIT bans new MAC address.

November 29, 2010: Beginning period for Count 5.

December 10, 2010: Swartz FOIAs "documents related to me, Aaron Swartz, as well as any documents related to any associated PACER investigation" from DOJ's Criminal Division; the FOIA returns no documents.

December 14, 2010: Beginning of period for which MIT handed over historical network flow data relating to IP addresses related to Swartz' laptop.

December 26, 2010: End of period for Count 5.

December 27, 2010: Beginning of period for Count 6.

November to December (probably November 29 through end of December):

> The indictment explains:
>
> During November and December, 2010, Swartz again used the "ghost laptop"

> (i.e., the Acer laptop) at MIT to download over two million documents from JSTOR,
>
> [snip]
>
> During this period, when Swartz connected to MIT's computer network, he circumvented MIT's guest registration process altogether. Rather than let MIT assign his computer an IP address automatically, Swartz instead simply hard-wired into the network and assigned himself two IP addresses. He did so by entering a restricted network interface closet in the basement of MIT's Building 16, plugging the computer directly into the network, and operating the computer to assign itself two IP addresses.
>
> The consolidated response describes:
>
> He also moderated the speed of the downloads, which made them less noticeable to JSTOR.
>
> [snip]
>
> Because the hacker had modified the speed of his downloads, JSTOR did not notice his latest downloads until Christmas. Now that MIT's network security had a more robust set of network tools, they could consult network traffic routing records and trace the IP address to a concrete physical location on campus.
>
> So on January 4, 2011, an MIT network security analyst traced the hacker's IP address to a network switch located in a basement wiring closet in MIT's Building 16.

January 4, 2011 (end of period for Count 6):

> The search warrant describes:

> Using network tools available to MIT on this occasion, the computer was tracked back to a specialized network wiring closet in the basement of Building 16 at MIT.
>
> The motion to suppress unwarranted searches describes:
>
> 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 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."
>
> [snip]

> 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.
>
> [snip]
>
> 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 laptop" for time periods including September and October of the previous year.
>
> [snip]
>
> 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 University6 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 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.
>
> The consolidated response describes:
>
> … an MIT network security analyst traced the hacker's IP address to a network switch located in a basement wiring closet in MIT's Building 16.
>
> [snip]
>
> When MIT personnel entered the closet, they found a cardboard box with a wire leading from it to a computer network switch.
>
> [snip]
>
> MIT called campus police to the scene, who, in turn, brought in the Cambridge Police and the Secret Service. over the course of the morning and early

> afternoon of January 4th, MIT and law enforcement officers collaboratively took several steps to identify the perpetrator and learn what he was up to:
>
> 1. *Cambridge Police crime scene specialists fingerprinted the laptop's interior and exterior and the external hard drive and its enclosure;*
> 2. *MIT placed and operated a video camera inside the closet, which, as discussed below, later recorded the hacker (subsequently identified as Aaron Swartz) entering the wiring closet and performing tasks within it;*
> 3. *The Secret Service opened the laptop and sought to make a copy of its volatile memory (RAM), which would automatically be destroyed when the laptop's power was turned off, but the effort resulted in their seeing only the laptop's user sign-in screen;*
> 4. *MIT connected a second laptop to the network*

> *switch in order to record the laptop's communications, a type of recording often referred to as a "packet capture;" the Secret Service subsequently concurred with the packet capture, none of which was turned over to officers until MIT was issued a subpoena after Swartz's arrest;*
>
> 5. *Beginning on January 4, 2011, MIT agreed to provide, and later provided, the Secret Service copies of network logs pertaining to the ghost laptop and ghost macbook between September 24, 2010 and January 6, 2011, some of which records were provided consensually, the remainder of which were provided pursuant to a subpoena to MIT.*

The law enforcement team replaced the scene as they had found it. Within an hour of their departure, Swartz entered the closet and swapped out the laptop and hard drive.

January 5, 2011: MA USAO begins separate investigation.

January 6, 2011: Swartz enters the closet again,

trying to hide his face from a camera, retrieves his computer, and then logs into MIT's network from the student center to assign his computer a new IP address and MAC address.

January 6, 2011, 2:00 PM: MIT Police Captain stopped Swartz on his bike and identified himself as a police officer.

January 6, 2011, 3:00 PM: "Law enforcement" find Swartz' laptop in MIT student center.

January 7, 2011: SS emails AUSA Stephen Heymann saying he is "prepared to take custody of the laptop … whenever you feel is appropriate. As far as I know n oone has sought a warrant for the examination of the computer" or other hardware. This email was turned over belatedly in discovery.

February 9, 2011: Secret Service obtain warrant to search Swartz' hardware and apartment, followed by a warrant to search his office.

February 11, 2011: Searches on house and office.

February 22, 2011: Hardware warrants expire.

February 24, 2011: Secret Service obtains new warrant for hardware.

February 28, 2011: Swartz FOIAs guidelines on Secret Service techniques for reading encrypted hard disks, as well as information on CERT's involvement in a prior case.

March 10, 2011: Swartz FOIAs "any policies, procedures, or guides for using data stored by Google for investigations, data-collection, and surveillance."

March 22, 2011: Swartz FOIAs "Any records requests made to Amazon and any responses from Amazon in connection with any such requests. This includes subpoenas, warrants, 2703 orders, National Security Letters, etc."

April 8, 2011: DHS/USSS provides initial responses (under separate cover) to both Swartz' Google FOIA explaining fees.

May 16, 2011: Swartz served with forfeiture warrant for four hard drives holding JSTOR materials.

May 21, 2011: DOJ responds to Swartz’ Amazon FOIA asking for more information.