BOS

From: BOS
Sent: Wednesday, June 29, 2011 9:40 AM
To: CID
Cc: ISD; BOS
Subject: CT 775.510 Aaron Swartz (102-775-60071-S)

U.S. SECRET SERVICE INVESTIGATIVE REPORT

FROM: BOSTON FIELD OFFICE
TO: CRIMINAL INVESTIGATIVE DIVISION
INFO: INVESTIGATIVE SUPPORT DIVISION

FILE: 102-775-60071-S
X-REF: N/A
SEIZURE#: N/A

SUBJECT: REPORT OF CONTINUING INVESTIGATION

ACTUAL LOSS: $TBD

POTENTIAL LOSS: $2,000,000.00

FILE COPY

CASE TITLE:	AARON SWARTZ
CASE TYPE:	775.510
SECONDARY TYPES:	848.191, 848.304, 848.930
CONTROLLING OFFICE:	BOSTON FIELD OFFICE
REPORT MADE BY:	SA (b)(6),(b)((b)(6),(b)((b)(6),(b)(7)(C)
DATE CASE OPENED:	01/07/11
PREVIOUS REPORT:	02/28/11
REPORTING PERIOD:	02/29/11 - 06/29/11
STATUS:	CONTINUED

SYNOPSIS:

Investigation has determined Aaron Swartz intruded into the MIT network without authorization by breaking into a locked telecommunications closet containing hardware for the MIT network, connecting a computer to the MIT network and downloading documents from JSTOR.

Case continued in Boston.

DETAILS OF INVESTIGATION:

Reference is made to all previous reports in this case, the most recent of which is a Request for Investigation Other District (IOD) written by SA (b)(6),(b)(on 02/28/11.

Reference is made to the Report of Investigation Other District written by SA (b)(6),(b)(of the San Francisco Field Office on 06/23/11.

Reference is made to the conference call between SA (b)(6),(b)(7)(C), AUSA Stephen Heymann, SA (b)(6),(b)(7)(and (b)(6),(b)(7)(C) from the Computer Emergency Response Team Coordination Center at Carnegie Mellon University on 03/09/11.

Reference is made to the conference call between SA (b)(6),(b)((b)(6),(b) (b)(6),(b AUSA Heymann, Detective of the Cambridge Police, and (b)(6),(b)(7)(C) of MIT on 06/20/11.

Reference is made to the conference call between SA (b)(6),(b)((b)(6),(b)(and (b)(6),(b)(7)(C) AUSA Heymann, and (b)(6),(from JSTOR on 06/25/11.

On 03/09/11, SA (b)(6) (b)(6),(b)(and SA (b)(6),(b)(7)(C) of the San Francisco Field Office interviewed (b)(6), (b)(6),(b at (b)(6),(b)(7)((b)(6),(b)(7)(C) (b)(6),(b)(7)(C) (b)(6),(b)((b)(6),(b)(7)(C (b)(6),(b)(7) The details of the interview are described in a Memorandum of Interview written by SA A copy of that MOI will be maintained in this case folder.

advised that she didn't have any contact, but did hear that due to his arrest, he was no longer allowed on the MIT campus. Due to this restriction, (b)(6),(b) advised that she heard Swartz was upset because he would not be permitted to participate in an annual campus wide scavenger hunt, of which he participates in every year. (b)(6),(b) was asked if Swartz ever mentioned JSTOR records to her, and (b)(6),(b) advised that she has never heard Schwarz discuss JSTOR records. Please see the Memorandum of Interview dated 3/9/11 for additional details.

On 6/7/11, I contacted SA (b)(6),(b) regarding the interview of (b)(6),(b)(SA (b)(6),(b)(advised he was preparing to indict Aaron Swartz and will consult with AUSA Heymann to determine if an interview with (b)(6),(b)(is necessary.

On 6/10/11, I was contacted by SA (b)(6),(b) who advised that after a discussion with AUSA Heymann the interview of (b) (b)(6),(b) (7)(C) would not be necessary.

Case closed in San Francisco.

JUDICIAL ACTION:

No Judicial Action is being sought in the Northern District of California at this time.

SUSPECTS/DEFENDANTS:

SWARTZ, Aaron H - SUSPECT
1599: Yes
1599A: No

(b)(6),(b)((b)(6),(b)(7)(C) - SUBJECT
AKA: (b)(6),(b)(7)(C)
RACE:
SEX:
DOB:
SSN: (b)(6),(b) (7)(C)
FBI:
SID:
HT:
WT:
EYES:
HAIR
1599: No
1599A: No
PHOTO: No
PRINTS: No
POB:
DL/STATE:
ADDRESS:
EMAIL: (b)(6),(b)(7)(C)
DATABASE CHECKS: 02/24/11

(b)(6),(b)(7)(C) - SUBJECT
AKA: N/A
RACE: (b)(6),(b)(7)(C)
SEX:
DOB:
SSN: (b)(6),(b)
FBI: N/A
SID: N/A
HT: N/A
WT: N/A
EYES: (b)(6),(b)(7)(C)
HAIR
1599: No

BOS

From: BOS
To: CID
Sent: Mon 2/28/2011 3:37 PM
Cc: ISD; SFO; BOS
Subject: 775.510 Request for Investigation Other District - Aaron Swartz (102-775-60071-S)
Attachments:

U.S. SECRET SERVICE INVESTIGATIVE REPORT

FROM: BOSTON FIELD OFFICE
TO: CRIMINAL INVESTIGATIVE DIVISION
SAN FRANCISCO FIELD OFFICE
INFO: INVESTIGATIVE SUPPORT DIVISION

FILE: 102-775-60071-S
X-REF: N/A
SEIZURE#: N/A

SUBJECT: REQUEST FOR INVESTIGATION OTHER DISTRICT

FILE COPY

ACTUAL LOSS: $ TBD

POTENTIAL LOSS: $ 2,000,000.00

CASE TITLE: AARON SWARTZ
CASE TYPE: 775.510
SECONDARY TYPES: 848.191, 848.304, 848.930
CONTROLLING OFFICE: BOSTON FIELD OFFICE
REPORT MADE BY: SA (b)(6),(b)(7)(C) (b)(6),(b)(7)(C)
DATE CASE OPENED: 01/07/11
PREVIOUS REPORT: 01/21/11 - OPENING REPORT
REPORTING PERIOD: 01/22/11 - 02/28/11
STATUS: CONTINUED

2011

SYNOPSIS:

Investigation has determined Aaron Swartz intruded into the MIT network without authorization by making entry into a locked closet containing networking components for MIT networks, connecting a computer to the MIT network, and downloading documents from JSTOR. Swartz was arrested by MIT Police and agents of the New England Electronic Crimes Task Force and charged with violation of Massachusetts General Law (MGL) for breaking and entering.

Agents and Detectives of the New England Electronic Task Force subsequently executed search warrants at Swartz's residence and office.

The San Francisco Field Office is requested to interview (b)(6),(b)(7)(C) two known associates of Swartz, to determine their knowledge of his activities.

Case continued in Boston.

DETAILS OF INVESTIGATION:

Reference is made to the Opening Report in this case, written by SA (b)(6),(b)(on 01/21/11.

On 01/25/11, SA (b)(6),(b)((b)(6),(b)(7)(C) the (b)(6),(b)(7)(C) (b)(6),(b) the from (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) (b)(6),(the (b)(6),(b)((b)(6),(b)(7)(C) for JSTOR, (b)(6),(b)(7) a (b)(6),(b)(7)(C) for JSTOR, and AUSA Stephen Heymann held a conference call. (b)(6),(b) confirmed that JSTOR has licensing agreements with publishers to make journals and articles available on the JSTOR web site, and that some of those licensing agreements include revenue sharing with publishers in which the publishers will get a share

of the fees JSTOR collects from institutions. (b)(6),(b) stated that some of the publishers allow for a direct fee to download an individual article, but some publishers do not want individual articles downloaded. (b)(6),(b) estimated that the value of the documents Swartz downloaded to be in excess of $2 million. (b)(6),(b) stated that he believed the average cost of the articles was $14.00. (b)(6),(stated that the first indication of an intrusion was a degradation of service for all customers. (b)(6), stated that the software on the JSTOR site relies on cookies to track users and that Swartz must have found a way to delete the JSTOR cookies from his system prior to making a new request to download a document. (b)(6),(b stated multiple download requests occurred simultaneously and that at times, hundreds of download requests were occurring concurrently. (b)(6),(b)(confirmed that the JSTOR terms and conditions clearly prohibited the kind of downloading Swartz was doing.

On 02/03/11, SA (b)(6),(b) and Detective (b)(6),(b) received the Acer Aspire netbook, hard drive enclosure, Western Digital hard drive contained in the enclosure, and a USB flash drive from MIT Police (b)(6),(b)(7)(C). SA (b)(6),(b)(and Detective (b)(6),(b) took the evidence items directly to Cambridge Police Headquarters. The evidence items were logged into Cambridge Police evidence and taken to the Cambridge Police Identification Unit. The Identification Unit began processing the items for fingerprints. The results of the analysis is pending.

On 02/04/11, SA (b)(6),(b)(Detective (b)(6),(b)(7)(C) of the Cambridge Police, (b)(6),((b)(6),(b) from the Massachusetts Institute of Technology, and AUSA Stephen Heymann held a conference call. (b)(6),(b) explained that he was driving to work on 01/04/11 when (b)(6),(b)(7)(C) called him and told him that he found a laptop connected to a switch. (b)(6),(b)(explained that previously (b)(6),(b)(7)(C) had sent an email to (b)(6),(b)(7) describing the switch he had traced the excessive downloading from JSTOR to. (b)(6),(b)(explained that after (b)(6),(b) found the laptop connected to the switch, he started a packet capture on the same switch. (b)(6),(b) also explained that the switch the laptop was connected to was an entry switch, and that normally only edge switches should be plugged into the entry switch. (b)(6),(b)(also explained that when (b)(6),(b)(7)(C) arrived, he used NMAP to discover that port 22 and 8092 were open on the laptop that was discovered. (b)(6),(b)(said that he reviewed the packet capture and discovered 14 different IP addresses sending SSH traffic to the laptop. (b)(6),(b) believed that some of the IP addresses were SSH background noise, however he did note that 18.181.0.232 could be traced to the linerva server at MIT. The linerva server is a Linux dial up server run by the Student Information Processing Board at MIT. (b)(6),(b)(7)(C) stated that he was still working on analyzing the packet capture.

On 02/07/11, (b)(6),(b)(7)(C) told SA (b)(6),(b)(7) that he noticed that on 01/06/11, the laptop used by Swartz was briefly registered on the MIT network from building 4 of MIT. (b)(6),(b)(7) noticed that during that time the laptop communicated with IP addresses 174.129.66.198, 204.236.212.151 and 50.16.222.69. (b)(6),(b)(7) stated that those IP addresses are associated with Amazon Elastic Compute Cloud, which is a web service that provides resizable compute capacity in the cloud.

Also on 02/07/11, (b)(6),(b)(7)(C) sent an email to AUSA Heymann to revise her estimate of how many documents were downloaded by Swartz. (b)(6),(b) stated that Swartz downloaded over 2.8 million documents in November and December of 2010. (b)(6),(b) also forwarded emails from (b)(6),(b)(7)(C) stating that the initial analysis of the activity indicated that the downloads were done systematically using sequential increases in stable URLs. The same email included a statement from (b)(6),(b)(7)(C) of JSTOR indicating that the downloading did not appear to be targeted towards research articles or any particular titles, collections, or disciplines. For the 2.8 million downloads in November and December of 2010, the breakdown was 1,385,569 research articles, 938,063 reviews, 62,127 news articles

INVENTORY MADE BY: SA (b)(6),(b)(
DESCRIPTION OF ITEMS: Apple iMac Model A1311 serial number W8025AXGD87
Western Digital Hard Drive SN WMANN1006724

SEIZED / OBTAINED FROM: Aaron Swartz
LOCATION: Boston Field Office Evidence Vault
DISPOSITION: Held pending judicial action.

EVIDENCE SSF 1544 S/N: 102 2011 CE 39
DATE OF INVENTORY: 02/25/11
INVENTORY MADE BY: SA (b)(6),(b)
DESCRIPTION OF ITEMS: Acer Aspire One SN LUSAX0000100110O1E1601
Rocketfish Enclosure with WD hard drive

WMAZA1626675

HP USB Drive marked 0045SMKBT1 85102

SEIZED / OBTAINED FROM: Cambridge Police
LOCATION: Boston Field Office Evidence Vault
DISPOSITION: Held pending judicial action.

DISPOSITION:

The San Francisco Field Office is requested to interview (b)(6),(b)(7)(C) and (b)(6),((b)(6),(b) to determine if Swartz discussed JSTOR or MIT with them, and if they had any knowledge of Swartz's downloading of documents from JSTOR. Prior to making contact with (b)(6),(b)(and (b)(6),(b) the San Francisco agent assigned this IOD is requested to contact Boston case agent (b)(6),(b)((b)(6),(b)(at (b)(6),(b)(7)(C) to further discuss this case.

Case continued pending further investigation and judicial action.

USSS / BOSTON (b)(6),(b)(7)(C) / RICCIARDI

BOS

From: BOS
To: CID
Cc: ISD; BOS
Subject: 775.510 Opening Report - Aaron Swartz (102-775-60071-S)
Attachments:
Sent: Fri 1/21/2011 2:58 PM

U.S. SECRET SERVICE INVESTIGATIVE REPORT

FROM: BOSTON FIELD OFFICE
TO: CRIMINAL INVESTIGATIVE DIVISION
INFO: INVESTIGATIVE SUPPORT DIVISION

FILE: 102-775-60071-S
X-REF: N/A
SEIZURE#: N/A

SUBJECT: OPENING REPORT

FILE COPY

CASE TITLE: AARON SWARTZ
CASE TYPE: 775.510
SECONDARY TYPES: 848.191, 848.304, 848.930
CONTROLLING OFFICE: BOSTON FIELD OFFICE
REPORT MADE BY: SA (b)(6),(b)(7)(C) (b)(6),(b)(7)(C)
DATE CASE OPENED: 01/07/11
PREVIOUS REPORT: N/A
REPORTING PERIOD: 01/04/11 - 01/21/11
STATUS: CONTINUED

SYNOPSIS:

On 01/04/11, MIT police requested assistance from members of the New England Electronic Crime Task Force regarding an investigation into a computer that was found in a locked closet at MIT and was connected to the MIT Network without authorization. Further investigation revealed that a subject later identified as Aaron Swartz, intruded into the MIT network without authorization by making entry into a locked closet containing networking components for MIT networks, connecting a computer to the MIT network, and downloading documents from JSTOR.

On 01/06/11, Aaron Swartz was arrested by MIT Police and agents of the New England Electronic Crimes Task Force and charged with violation of Massachusetts General Law (MGL) for breaking and entering. The investigation of Swartz's unauthorized intrusion into the MIT network and the theft of documents from JSTOR continue.

Case continued in Boston.

DETAILS OF INVESTIGATION:

On 01/04/11, Detective (b)(6),(b)(7)(C) of the Cambridge, MA Police Department and a member of the New England Electronic Crimes Task Force, received a call from (b)(6),(b)(7) (b)(6),(b)(7)(C) (b)(6),(b)(7)(C @MIT.EDU) of the Massachusetts Institute of Technology (MIT) Police Department, informing him that an unauthorized computer had been found in a wire closet on MIT grounds and that Network Traffic suggested that the computer was being used to download expensive technical journals without authorization. The computer was found in a wire closet in the basement of Building 16, the Dorrance Building (77 Massachusetts Avenue, Cambridge, MA) which houses the MIT Biological Engineering Department.

Continuing on 01/04/11, SA (b)(6),(b)(7)(C) Detective (b)(6),(b (b)(6),(and Detective (b)(6),(b)((b)(6),(b)(7 of the Boston Police Department, traveled to MIT and met with (b)(6),(b)(7) (b)(6),((b)(6),(b)(7) and (b)(6),(b)(7)(C) a (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) (b)(6),(b)(7)(C)

(b)(6),(b)(7) for MIT, 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 LUSAX0D001001100E1601. 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)(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) (b)(6),(b)(7)(C) (b)(6), (b)(6),(b)(7) regarding excessive downloading from two IP addresses 18.55.6.216 and 18.55.6.215. JSTOR restored MIT access but blocked access to the identified IP addresses. (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) (b)(6),(b)(7)(mit.edu), (b)(6),(b)(7)(C), 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)(7 disabled the computer registration.

On 10/09/10, (b)(6),(b)(7)(C) from JSTOR (b)(6),(b)(7)(C) emailed (b)(6) (b)(6),(b)(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)(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)(C) (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) (b)(6),(b)(7) for MIT, notified (b)(6),(b)(7) and (b)(6),(b)(7)(C the (b)(6),(b)(7)(C) MIT (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) 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.

On 01/03/11, (b)(6),(b)(received an email from (b)(6),(b)(7)(forwarded from (b)(6),(b) informing him that that the excessive downloading of journals had begun again.

On 01/04/11, (b)(6),(b)(emailed (b)(6),(b)(7)(C) the (b)(6),(b)(7)(C) Operations, and (b)(6),(b)(7)(C) (b)(6),(b)(7)(C), (b)(6)@mit.edu) (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) for MIT, asking them to further pinpoint the location of the computer downloading the journals. At 0808, (b)(6),(b)(located a computer hidden by a box connected to a switch in a wire closet in the basement of building 16. The computer was also connected to an external hard drive. (b)(6),(b established a packet capture of the same switch the computer was found attached to.

(b)(6),(b)(also provided SA (b)(6),(b)(with a copy of historical network flow data concerning IP addresses 18.55.6.240 and 18.55.7.240 from 12/14/10 to 01/04/11 and DHCP log information for computers registered as ghost-macbook and ghost-laptop.

SA (b)(6),(b) contacted SA (b)(6),(b)(7)((CID) at the CERT Coordination Center at the Software Engineering Institute at Carnegie Mellon University. SA (b)(6),(b)(with instructions to upload the data to the CERT drop box. SA (b)(6) provided SA

On 01/06/11, at approximately 1232, video surveillance showed the individual later identified as Swartz return to the wire closet and remove the netbook and external hard drive. Later, (b)(6),(b)(7) (b)(6),(b)(7)(C) of the MIT Police Department called (b)(6),(b)(7) (b)(6),(b)(of the MIT Police Department and stated that he had located the suspect later identified as Swartz riding his bicycle on Massachusetts Avenue near the intersection with Lee Street in Cambridge, Massachusetts. (b)(6),(b)(7) (b)(6),(b)(and SA (b)(6),(b)(responded to Lee Street to assist Captain (b)(6),(b)((b)(6),(b)(7) (b)(6),(b) attempted to interview Swartz, however Swartz jumped off of his bicycle and ran down Lee Street. (b)(6),(b)(7)((b)(6),(b)(and SA (b)(6),(b) detained the suspect and he was subsequently placed under arrest. A search of the backpack the suspect was wearing revealed a U.S. passport in the name of Aaron Swartz and one (1) USB Thumb Drive. No computer was found in the backpack. Swartz was transported by Cambridge Police to Cambridge Police headquarters and subsequently charged with violation of Massachusetts General Law (MGL) for Breaking and Entering.

Also on 01/06/11, (b)(6),(b)(checked the DHCP logs for computer registrations containing the word "ghost". Ghost-laptop was identified as still being active on the MIT network using the same MAC address as used on 01/04/11 to download journals. (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) (b)(6),(b)(7)(@mit.edu) an MIT Network Engineer, traced ghost-laptop on the network to building W20 on the 5th floor. MIT Building W20 is the Stratton Student Center. (b)(6),(b)((b)(6),(b)(and (b)(6),(b traveled to the Stratton Student Center and determined that the network drop location ghost-laptop connected to was the Student Information Processing Board office, room 557. (b)(6),(b)(contacted (b)(6),(b)(7) (b)(6),(b)(to inform him that they had traced the netbook to a room in the student center. SA (b)(6),(b) met (b)(6),(b)(and (b)(6),(b) at the student center and found the Acer Aspire netbook and external hard drive unattended, under a table, powered on and connected to the MIT network by a cable. Using gloves, SA (b)(6),(b)(examined the netbook. The netbook appeared to be frozen halfway in the shutdown state and all attempts to access a terminal on the machine were unsuccessful. It 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. The laptop was placed in an evidence bag and turned over to MIT Police to be inventoried into evidence.

Continuing on 01/06/11, SA (b)(6),(b) and (b)(6),(b)(7) (b)(6),(b)(traveled to Cambridge Police Headquarters to interview Swartz. At Cambridge Readquarters, SA (b)(6),(b)(met (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) (b)(6),(b)(7) (b)(6),(b)(7)((b)(6),((b)(6),(b)(informed SA (b)(6),(b) that he represented Swartz and that his client would not make a statement. Swartz was not cooperative with investigators. Swartz initially refused to provide his name, date of birth and other biographical information.

On 01/10/11, SA (b)(6),(b)(7 AUSA Heymann and (b)(6),(b)(7)(C) from JSTOR conducted a conference call to discuss the theft of material from JSTOR.

On 01/14/11, SA (b)(6),(b)(Detective (b)(6),(b) (b)(6),(b)(7)((b)(6),(b)(7)(C) and AUSA Heymann met at the MIT office of General Counsel with (b)(6),(b)(7)(C) counsel for MIT.

JUDICIAL ACTION:

On 01/06/11, Aaron Swartz was arrested by MIT Police Department and charged with violation of Massachusetts General Law (MGL) Chapter 266, Section 18, Breaking and Entering.

On 01/06/11, SA (b)(6),(b) contacted AUSA Steven Heymann, District of Massachusetts, to brief him on the above investigation.

On 01/07/11, Aaron Swartz was arraigned in Cambridge, MA District Court for violation of MGL Chapter 266, Section 18, Breaking and Entering. The case was assigned docket number 1152CR0073.

SUSPECTS / DEFENDANTS:

SWARTZ, Aaron H. - SUSPECT

AKA:	N/A
RACE:	White
SEX:	Male
DOB:	11/08/1986
SSN:	(b)(6),(b)(-1374
FBI:	675304KD0
SID:	MA10556539
HT:	5' - 06"
WT:	120 lbs.
EYES:	Brown
HAIR	Brown
1599:	Yes
1599A:	No
PHOTO:	Yes
PRINTS:	Yes
POB:	Chicago, IL
DL/STATE:	
ADDRESS:	
EMAIL:	
DATABASE CHECKS:	01/07/11

EXAMS CONDUCTED:

ECSAP:	Pending
POLY:	N/A
FSD:	N/A

DATABASE SEARCHES CONDUCTED:

MCI / CI: 01/07/11
NCIC/NLETS: 01/07/11
CCS/CFT: 01/07/11
LOCAL LE: 01/07/11

EVIDENCE / CONTRABAND / PERSONAL PROPERTY:

All evidence in this case is currently being held at MIT Police Headquarters.

DISPOSITION:

Case continued pending further investigation and judicial action.

USSS / BOSTON (b)(6),(b)(7)(C) RICCIARDI

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	**Crim. No.** 11-cr-10260
v.	**VIOLATIONS:**
AARON SWARTZ,	**18 U.S.C. § 1343 (Wire Fraud)**
Defendant	**18 U.S.C. § 1030(a)(4) (Computer Fraud)**
	18 U.S.C. § 1030(a)(2), (c)(2)(B)(iii) (Unlawfully Obtaining Information from a Protected Computer)
	18 U.S.C. § 1030(a)(5)(B), (c)(4)(A)(i)(I),(VI) (Recklessly Damaging a Protected Computer)
	18 U.S.C. § 2 (Aiding and Abetting)
	18 U.S.C. § 981(a)(1)(C), 28 U.S.C. § 2461(c), and 18 U.S.C. §982(a)(2)(B) (Criminal Forfeiture)

2011

INDICTMENT

The Grand Jury charges that at all relevant times:

PARTIES

1. The Massachusetts Institute of Technology ("MIT") was and continued to be a leading research and teaching university located in Cambridge, Massachusetts.

2. JSTOR, founded in 1995, was and continued to be a United States-based, not-for-profit organization that provides an online system for archiving and providing access to academic journals. It provides searchable digitized copies of over 1,000 academic journals, dating back for lengthy periods of time.

3. JSTOR's service is important to research institutions and universities because it can be extraordinarily expensive, in terms of both cost and space, for a research or university library to maintain a comprehensive collection of academic journals. By digitizing extensive, historical collections of journals, JSTOR enables libraries to outsource the journals' storage,

RIF

ensures their preservation, and enables authorized users to conduct full-text, cross-disciplinary searches of them. JSTOR has invested millions of dollars in obtaining and digitizing the journal articles that it makes available as part of its service.

4. JSTOR generally charges libraries, universities, and publishers a subscription fee for access to JSTOR's digitized journals. For a large research university, this annual subscription fee for JSTOR's various collections of content can cost more than $50,000. Portions of the subscription fees are shared with the journal publishers who hold the original copyrights. In addition, JSTOR makes some articles available for individual purchase. Publishers decide which articles can be purchased individually and set fees for their articles. JSTOR facilitates the purchase of these articles from the archive on behalf of the participating publishers.

5. JSTOR did not permit users:

a. to download or export content from its computer servers with automated computer programs such as web robots, spiders and scrapers;

b. to download all of the articles from any particular issue of a journal; or

c. to make other than personal use of individually downloaded articles.

6. JSTOR notified its users of these rules, and users accepted these rules when they chose to obtain and use JSTOR's content.

7. JSTOR provided MIT with its services and content for a fee.

8. MIT, in turn, made JSTOR's services and content available to its students, faculty, and employees. MIT also allowed guests of the Institute to have the same access as its students, faculty, and employees for short periods of time while they were on campus.

9. JSTOR's computers were located outside the Commonwealth of Massachusetts, and thus any communications between JSTOR's computers and MIT's computers in Massachusetts crossed state boundaries. JSTOR's computers were also used in and affected interstate and foreign commerce.

10. Aaron Swartz lived in the District of Massachusetts and was a fellow at Harvard

RIF

University's Center for Ethics. Although Harvard provided Swartz access to JSTOR's services and archive as needed for his research, Swartz used MIT's computer networks to steal well over 4,000,000 articles from JSTOR. Swartz was not affiliated with MIT as a student, faculty member, or employee or in any other manner other than his and MIT's common location in Cambridge. Nor was Swartz affiliated in any way with JSTOR.

OVERVIEW OF THE OFFENSES

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

a. break into a restricted computer wiring closet at MIT;

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

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

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

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

f. elude detection and identification;

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

MEANS OF COMMITTING THE OFFENSES

12. Swartz alone, or in knowing concert with others unknown to the grand jury, (hereafter simply "Swartz" in this section) committed these offenses through the means described below.

September 24 through 27, 2010

13. On September 24, 2010, Swartz purchased an Acer laptop computer from a local

RIF

computer store with the intent of using it to automatically and systematically harvest JSTOR's archive of digitized journal articles.

14. Later that day, Swartz connected the Acer computer to MIT's computer network from a location in Building 16 at MIT and registered under a pseudonym with MIT's computer network as a guest. MIT offers campus guests short-term service on its computer network. Campus guests must register on the MIT network and are limited to a total of fourteen days per year of network service.

15. Swartz registered on the network using identifiers chosen to hide his identity as the computer's owner and user.

a. The computer was registered under the fictitious guest name "Gary Host."

b. The computer's client name was specified as "ghost laptop." A computer's client name helps to identify it on a network and can be chosen by its user. In this case, the name was simply created by abridging the pseudonym "Gary Host," combining the first initial "g" with the last name "host."

c. The fictitious "Gary Host's" e-mail address was identified as "ghost@mailinator.com." This was a "throwaway" e-mail address. Mailinator is a free, disposable e-mail service that allows a user to create a new e-mail address as needed, without even registering the address with Mailinator. Mailinator provides this service for users to have an anonymous and temporary e-mail address. Mailinator accepts mail for any e-mail address directed to the mailinator.com domain without need for a prior registration, and it allows anyone in the world to read that mail without having to create an account or enter a password. All mail sent to mailinator.com is automatically deleted after several hours whether read or not.

16. On September 25, 2010, Swartz used the Acer laptop to systematically access and rapidly download an extraordinary volume of articles from JSTOR. He used a software program

RIF

to automate the downloading process so that a human being would not need to keep typing in the archive requests. The program was also designed to sidestep or confuse JSTOR's efforts to prevent this behavior.

17. These rapid and massive downloads and download requests impaired computers used by JSTOR to service client research institutions and threatened to misappropriate its archive.

18. As JSTOR, and then MIT, became aware of these efforts to steal a vast proportion of JSTOR's archive, each took steps to block the flow of articles to Swartz's computer and thus to prevent him from redistributing them. Swartz, in turn, repeatedly altered the appearance of his Acer laptop and the apparent source of his automated demands to get around JSTOR's and MIT's blocks against his computer.

a. On the evening of September 25, 2010, JSTOR blocked the computer's access to its network by refusing communications from the computer's assigned IP address. An IP (short for "Internet Protocol") address is a unique numeric address used by a computer on the Internet. Every computer attached to the Internet must be assigned an IP address so the Internet traffic sent from and directed to that computer can be directed properly from the source to its destination. Most Internet service providers control a range of IP Addresses. MIT controls all IP addresses that begin with the number 18. In this case, the computer had been assigned an IP address of 18.55.6.215, and JSTOR blocked communications from that IP address.

b. On September 26, 2010, Swartz obtained for his computer a new IP address on the MIT network – 18.55.6.216 – and began again to download an extraordinary volume of articles from JSTOR. Accesses from this address continued until the middle of the day, when JSTOR spotted and blocked this IP address as well. Because the exploits on September 25 and 26 were both

RIF

launched from MIT IP addresses beginning with 18.55.6 , and because computers used by JSTOR to service client research institutions were again impaired and its archive at risk of misappropriation, on September 26, 2010, JSTOR began blocking a much broader range of IP addresses. As a result, legitimate JSTOR users at MIT were denied access to JSTOR's archive until September 29, 2010.

c. Notified by JSTOR of what was happening, MIT sought to block Swartz more specifically. It did so by prohibiting the Acer laptop from being assigned an IP address on MIT's network. When a user plugs his computer into the wired network on MIT's campus, his computer's MAC address is used to determine whether he has been authorized to use the network. A MAC address is a unique identifier assigned to a computer network interface, in this case, the Acer laptop's network interface card. A MAC address most often is assigned by the manufacturer of the network interface card and therefore generally remains constant on the device. Although a MAC address is intended to be a permanent and globally unique identification, a user with the right knowledge can change the MAC address, an action referred to as "MAC address spoofing," as discussed below.

d. As part of the registration process, "Gary Host's" computer, i.e., the Acer laptop, had identified its network interface's MAC address as 00:23:5a:73:5f:fb. Consequently, on September 27, 2010, MIT deactivated the guest registration for the "ghost laptop" by barring any network interface with that MAC address from being assigned a new IP address.

19. MIT banned the Acer laptop from its network under and consistent with its own computer use rules, which required users to:

a. use the network to support MIT's research, education, and MIT administrative activities, or at least to not interfere with these activities;

b. maintain the system's security and conform to applicable laws, including copyright laws; and

c. conform with rules imposed by any networks to which users connected through MIT's system.

Guest users of the MIT network agreed to be bound by the same rules that applied to students, faculty, and employees. These rules explicitly notified users that violations could lead to state or federal prosecution.

October 2 through 9, 2010

20. Despite knowing that his computer had been blocked from JSTOR's and MIT's networks, Swartz sought and obtained another guest connection on MIT's network, again for his Acer laptop less than a week later, on October 2, 2010.

21. Once again, Swartz registered the Acer latop on the network using identifiers chosen to avoid identifying Swartz as the computer's owner and user:

a. The computer was once again registered under the fictitious name "Gary Host" and the client name "ghost laptop."

b. To evade the MAC address block, Swartz spoofed the computer's MAC address, manipulating it from 00:23:5a:73:5f:fb to 00:23:5a:73:5f:fc (the final "b" became a "c").

c. By re-registering the "ghost laptop," Swartz ensured that it was assigned a new IP address. By obtaining a new IP address, Swartz disassociated his rogue computer from the IP addresses used to exploit JSTOR in September.

22. On October 8, 2010, Swartz connected a second computer to MIT's network and registered as a guest, using similar naming conventions: the computer was registered under the name "Grace Host," the computer client name "ghost macbook," and the throw-away e-mail address "ghost42@mailinator.com."

23. The next day, October 9, 2010, Swartz used both the "ghost laptop" and the

"ghost macbook" to systematically and rapidly access and download an extraordinary volume of articles from JSTOR. The pace was so fast that it brought down some of JSTOR's computer servers.

24. In response, JSTOR blocked the entire MIT computer network's access to JSTOR for several days, beginning on or about October 9, 2010.

November and December, 2010

25. During November and December, 2010, Swartz used the "ghost laptop" (i.e., the Acer laptop) at MIT to make over two million downloads from JSTOR. This is more than one hundred times the number of downloads during the same period by all the legitimate MIT JSTOR users combined. Of the downloads, approximately half were research articles, with the remainder being reviews, news, editorials, and miscellaneous documents.

26. This time around, Swartz circumvented MIT's guest registration process altogether when he connected to MIT's computer network. By this point, Swartz was familiar with the IP addresses available to be assigned at the switch in the restricted network interface closet in the basement of MIT's Building 16. Swartz simply hard-wired into the network and assigned himself two IP addresses. He hid the Acer laptop and a succession of external storage drives under a box in the closet, so that they would not be obvious to anyone who might enter the closet.

January 4 through 6, 2011

27. On January 4, 2011, Aaron Swartz was observed entering the restricted basement network wiring closet to replace an external hard drive attached to his computer.

28. On January 6, 2011, Swartz returned to the wiring closet to remove his computer equipment. This time he attempted to evade identification at the entrance to the restricted area. As Swartz entered the wiring closet, he held his bicycle helmet like a mask to shield his face, looking through ventilation holes in the helmet. Swartz then removed his computer equipment from the closet, put it in his backpack, and left, again masking his face with the bicycle helmet

before peering through a crack in the double doors and cautiously stepping out.

29. Shortly thereafter, Swartz connected the Acer latop to MIT's network in a different building, again registering on the network using identifiers chosen to avoid identifying Swartz as the computer's owner and user.

a. The computer was registered under the fictitious name "Grace Host" and the client name "ghost laptop."

b. To evade the block on the computer's MAC address, Swartz had spoofed (manipulated) its MAC address a second time, changing it from the blocked 00:23:5a:73:5f:fb to 00:4c:e5:a0:c7:56.

c. By re-registering the "ghost laptop," Swartz ensured that it was assigned a new IP address. By obtaining a new IP address for his rogue computer, Swartz disassociated it from the IP addresses used to exploit JSTOR up to that point.

30. Swartz had a software program named "keepgrabbing.py" installed on the Acer laptop. Keepgrabbing.py was designed to download .pdf files from jstor.org and sidestep or confuse JSTOR's efforts to prevent the behavior.

31. When MIT Police spotted Swartz on the afternoon of January 6, 2011 and attempted to question him, he fled with a USB drive that contained the program "keepgrabbing2.py." "Keepgrabbing2.py" had distinct similarities to "keepgrabbing.py."

32. In all, Swartz stole approximately 4.8 million articles, a major portion of the total archive in which JSTOR had invested. Of these, approximately 1.7 million were made available by independent publishers for purchase through JSTOR's Publisher Sales Service.

33. Swartz intended to distribute a significant portion of JSTOR's archive of digitized journal articles through one or more file-sharing sites.

RIF

COUNT 1
Wire Fraud
18 U.S.C. §§ 1343 & 2

34. The Grand Jury realleges and incorporates by reference the allegations in paragraphs 1-33 of this Indictment and charges that:

From on or about September 24, 2010, through January 6, 2011, or thereabout, in the District of Massachusetts and elsewhere, the defendant,

AARON SWARTZ,

having devised and intended to devise a scheme and artifice to defraud and for obtaining property — namely, journal articles digitized and distributed by JSTOR, and copies thereof — by means of material false and fraudulent pretenses, representations, and promises, transmitted and caused to be transmitted by means of wire communication in interstate commerce writings, signs, signals, and pictures — namely, communications to and from JSTOR's computer servers — for the purpose of executing the scheme, and aided and abetted the same.

All in violation of Title 18, United States Code, Sections 1343 and 2.

COUNT 2
Computer Fraud
18 U.S.C. §§ 1030(a)(4) & 2

35. The Grand Jury realleges and incorporates by reference the allegations in paragraphs 1-33 of this Indictment and charges that:

From on or about September 24, 2010, through January 6, 2011, or thereabout, in the District of Massachusetts and elsewhere, the defendant,

AARON SWARTZ,

knowingly and with intent to defraud, accessed a protected computer — namely, a computer on MIT's network and a computer on JSTOR's network — without authorization and in excess of authorized access, and by means of such conduct furthered the intended fraud and obtained things of value — namely, digitized journal articles from JSTOR's archive — and aided and abetted the same.

All in violation of Title 18, United States Code, Sections 1030(a)(4) and 2.

RIF
2

COUNT 3
Unlawfully Obtaining Information from a Protected Computer
18 U.S.C. §§ 1030(a)(2), (c)(2)(B)(iii) & 2

36. The Grand Jury realleges and incorporates by reference the allegations in paragraphs 1-33 of this Indictment and charges that:

From on or about September 24, 2010, through January 6, 2011, or thereabout, in the District of Massachusetts and elsewhere, the defendant,

AARON SWARTZ,

intentionally accessed a computer — namely, a computer on MIT's computer network and a computer on JSTOR's network — without authorization and in excess of authorized access, and thereby obtained from a protected computer information whose value exceeded $5,000 — namely, digitized journal articles from JSTOR's archive — and aided and abetted the same.

All in violation of 18 U.S.C. §§ 1030(a)(2), (c)(2)(B)(iii) and 2.

RIF

COUNT 4
Recklessly Damaging a Protected Computer
18 U.S.C. §§ 1030(a)(5)(B), (c)(4)(A)(i)(I),(VI) & 2

37. The Grand Jury realleges and incorporates by reference the allegations in paragraphs 1-33 of this Indictment and charges that:

From on or about September 24, 2010, through January 6, 2011, or thereabout, in the District of Massachusetts and elsewhere, the defendant,

AARON SWARTZ,

intentionally accessed a protected computer — namely, a computer on MIT's computer network and a computer on JSTOR's network — without authorization, and as a result of such conduct recklessly caused damage to MIT and JSTOR, and, during a 1-year period, caused loss aggregating at least $5,000 in value and damage affecting at least 10 protected computers, and aided and abetted the same.

All in violation of Title 18, United States Code, Sections 1030(a)(5)(B), (c)(4)(A)(i)(I),(VI) & 2.

RIF
24

UNITED STATES GOVERNMENT

Memorandum of interview

U.S. Secret Service

Case # 102-775-60071-S

DATE AND TIME: March 9, 2011

LOCATION: (b)(6),(b)(7)(C)

SUBJECT INTERVIEWED: (b)(6),(b)(7)(C)

IN ATTENDANCE: SA (b)(6),(b)(7)(C) (SFO)
SA (b)(6),(b)(7)(C) (SFO)

On March 9, 2011, (b)(6),(b)(7)(C) was interviewed at (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) in reference to the Boston Field Office case number 102-775-60071-S. The interview was conducted by Agent (b)(6),(b)(7)(C) and Agent (b)(6),(b)(7)(C), San Francisco Field Office. During the interview (b)(6),(b)(7)(C) was asked about Aaron Schwarz and any information she had regarding his recent arrest. The following is a summary of her statements:

(b)(6),(b)(7)(C) stated that she is the kind of friend that does not ask questions when a friend asks for help. (b)(6),(b)(7)(C) elaborated by stating that she received a phone call from Schwarz, who asked her to call his lawyer and arrange bail for him, which she did.

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

When (b)(6),(b)(7)(C) was asked about any additional contact with Schwarz, she advised that she didn't have any contact, but did hear that due to his arrest, he was no longer allowed on the MIT campus. Due to this restriction, (b)(6),(b)(7)(C) advised that she heard Schwarz was upset because he would not be permitted to participate in an annual campus wide scavenger hunt, of which he participates in every year. (b)(6),(b)(7)(C) was asked if Schwarz ever mentioned JSTOR records to her, of which she advised that she didn't know what JSTOR was and asked for an explanation. Once JSTOR was explained in more detail, (b)(6),(b)(7)(C) advised that she believes that she may have access to those records (b)(6),(b)(7)(C) (b)(6),(b)(7)(C), but has never heard Schwarz discuss JSTOR records.

During the course of the interview, (b)(6),(b)(7)(C) was fully cooperative and openly answered any questions that were asked of her. (b)(6),(b)(7)(C) stated that she would fully cooperate in this investigation, and stated that if she hears from Schwarz, that she would contact Agent (b)(6),(b)(7)(C) who provided his contact information at the conclusion of the interview.

UNITED STATES GOVERNMENT

Memorandum of interview

U.S. Secret Service

Case # 102-775-60071-S

DATE AND TIME: April 13, 2011

LOCATION: 1 Courthouse Way, Boston, MA 02210

SUBJECT INTERVIEWED: (b)(6),(b)(7)(C)

IN ATTENDANCE: SA (b)(6),(b)(7)(C) (BOS)
Detective (b)(6),(b)(7)(C) Cambridge Police
AUSA Stephen Heymann
(b)(6),(b)(7)(C)

On April 13, 2011, (b)(6),(b)(7)(C) was interviewed at the John Joseph Moakley U.S. Courthouse at 1 Courthouse Way, Boston Massachusetts, in reference to the Boston Field Office case number 102-775-60071-S. The interview was conducted by Agent (b)(6),(b)(7)(C) and Cambridge Police Detective (b)(6),(b)(7)(C) and Assistant U.S. Attorney Stephen Heymann. Also in attendance were (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) attorneys with Fish and Richardson Professional Corporation. The following is a summary of her statements:

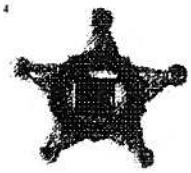
(b)(5),(b)(7)(C)

(b)(6),(b)(7)(C) she received a call from Swartz and that he told her he had been arrested. (b)(6),(b)(7)(C) said that she did not want to know why he had been arrested and that she was concerned about how he was emotionally. (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) said that (b)(6),(b)(7)(C) posted bail for Swartz. (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) the he had met Swartz before. (b)(6),(b)(7)(C) said that the main part of the discussion was regarding Swartz's mental health and that Swartz has had some depression problems. (b)(6),(b)(7)(C) said that she remembered Swartz mentioning something about a computer and something about Massachusetts Institute of Technology.

(b)(6),(b)(7)(C) said that after she spoke with Swartz she called one of her friends, (b)(6),(b)(7)(C) (b)(6),(b)(7)(C)

(b)(6),(b)(7)(C) said that Swartz did not like to have a computer at his house but that he had an office at the democracy center. (b)(6),(b)(7)(C) said that she thought that Swartz generally used Mac equipment.

(b)(6),(b)(7)(C) said that she understood that Swartz did something with JSTOR. (b)(6),(b)(7)(C) said that she believed that academic publishing is despised by academics (b)(6),(b)(7)(C) said that researchers have to pay to be published and then people have to pay to have access to the works.



Electronic Crimes Special Agent Program

CASE NUMBER: 102-866-0060071

CASE TITLE: Swartz

CITY OF OFFENSE: Cambridge

STATE OF OFFENSE: MA

CASE OFFICE: BOS (102)

TOTAL MEDIA PROCESSED: 9.30 TB

SUBJECT: Swartz, Aaron

IOD: N

REQUESTER: AUSA Heymann

EXAMINER'S SUPERVISOR: (b)(6) (b)(7)(C)

EXAMINER'S OFFICE: BOS (102)

DATES/APPROVERS

EXAM DATE: 07/07/2011

SUBMIT DATE: 07/26/2011

APPROVED DATE: 07/27/2011

USSS CASE INFORMATION

J-CASE:

S-CASE: S

OCCURRENCE: NOT SPECIFIED

SSF-1544: 102 2011 CE 39

INTERNAL TRACKING NUM:

ICR:

2011

OTHER AGENCY INFORMATION

OTHER AGENCY: N

OTHER AGENCY NO:

REQUESTOR:

REQUESTOR NUMBER:

CASE ENCRYPTION

ENCRYPTION USED: N

ENCRYPTION DESCR: NOT SPECIFIED

COMMENTS

CASE SUMMARY: Aaron Swartz broke into a network closet in MIT, attached a laptop to the MIT network and illegally downloaded a large number of documents from JSTOR.

DISPOSITION EVIDENCE: Held in the Boston Field Office pending judicial action

CASE TYPES

PRIMARY CASE TYPE: 866.775 - Computer Crime Investigations

SECONDARY CASE TYPES: 848.193 - Financial Crimes Task Forces
848.191 - Electronic Crimes Task Force
848.930 - Crimes Involving use of Emerging Technology
848.304 - Books/Poems/Plays

INVESTIGATIVE TOOLS

(b)(6) (b)(7)(C) Office: BOSTON FIELD OFFICE Agent Phone (b)(6) (b)(7)(C)

Approved by CID on 07/27/2011