

This document is made available through the declassification efforts
and research of John Greenewald, Jr., creator of:

The Black Vault



The Black Vault is the largest online Freedom of Information Act (FOIA) document clearinghouse in the world. The research efforts here are responsible for the declassification of hundreds of thousands of pages released by the U.S. Government & Military.

Discover the Truth at: <http://www.theblackvault.com>

work on Affidavit

Re: SSU

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

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

on BOF for Swartz

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

1374 on Cambridge PD Bookings

Call

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

Call

Wed or Thur

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

1/19/11 Conf Call

Key Points

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

Heymann talked to
yesterday 1/18/11
a brief direct contact w/ MIT

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

Pres out
w/ traffic out
SSH cannot link established

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

= BOF SSU = Accurate

ZZ Sec 101

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

RELEASE

Memorandum

United States Attorney
District of Massachusetts



Subject Re: Filter Team Instructions Concerning Search of IMac Model A1311, Serial number WB025AXGD87, Western Digital Hard Drive Model WD1200, Serial number WMANN1006724 and Sony Micro Vault USB Drive marked SDK USM 8GH(B)	Date February 18, 2011
To AUSA (b)(6),(b)(7)(C) Special Agent (b)(6),(b)(7)(C) Forensic Agents	From AUSA Stephen P. Heymann 

As we understand it, Aaron Swartz retained attorney Philip Cormier on January 6, 2011, following his arrest for breaking and entering at MIT. As a consequence, it is possible that communications between Swartz and Cormier, the law firm Good and Cormier, or Cormier's partner, Andrew Good, may be stored on the iMac computer, the Western Digital hard drive, and/or the Sony USB drive which we seized pursuant to search warrants on February 11, 2011. To minimize the chance that members of the investigative team will be exposed to attorney/client communications pertaining to that state case, we are implementing the following filtering protocol. AUSA (b)(6),(b)(7)(C) who is otherwise not involved in any manner with the investigation will be available to answer any questions. His telephone number is (b)(6),(b)(7)(C)

Forensic agents not otherwise involved in any aspect of the main investigation will conduct an initial review of the seized iMac, Western Digital hard drive and USB drive. It will be their task to identify and filter-out any attorney/client communications to the fullest extent

practicable. Towards this end, the filter team will conduct an initial search of the computer and two drives for the following terms:

goodcormier
agood
pcormier
Andrew Good
Mr. Good

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

Andrew
Philip Cormier
Mr. Cormier

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

Philip

The filter team will then examine each of the documents, records and e-mails ("the objects") containing one of these terms only to the extent necessary to establish if it contains an attorney/client communication. If the object does, the filter team will determine the object's hash value and add the hash value to a filter set. Agents involved with the investigation will use this hash set to filter out objects containing attorney/client communications prior to their search, examination and analysis of the computer and drives.

The hash value set should be preserved, should it be needed at a later point in the case.

COMMONWEALTH OF MASSACHUSETTS

MIDDLESEX, SS.

**SUPERIOR COURT DEPARTMENT
DOCKET NO. 2011-_____**

COMMONWEALTH

v.

AARON SWARTZ

COMMONWEALTH'S STATEMENT OF THE CASE

Now comes the Commonwealth in the above-captioned matter and submits this statement of the case. This statement is provided to assist the court and is not intended to be a bill of particulars nor does it contain all information known to the Commonwealth at this time.

JSTOR is a not-for-profit business which provides, for a fee, electronic access to a wide variety of academic journals. One of JSTOR's paying subscribers was the Massachusetts Institute of Technology ("MIT"), which in turn provided its faculty, students and guests limited access to JSTOR's archives. Mass downloading by automated means was specifically prohibited by the terms of MIT's agreement with JSTOR. On September 24, 2010, Aaron Swartz ("Swartz"), an expert in computer technologies and Internet communication, purchased an Acer laptop computer. Though he already owned a powerful laptop computer which was fully capable of accessing academic articles from the internet, he purchased this new computer because it would be more difficult to trace to him personally. He did so with the intent to download massive quantities of data from JSTOR's archives, with the intent to publish it in the public



domain and thus destroy JSTOR's business model. Though Swartz was affiliated with Harvard University, and thus had access to whatever academic articles he might have desired for his own research, Swartz instead endeavored to access the database through MIT, with which he had no affiliation, using an internet identity that would be difficult to identify.

He created a fictitious guest identity ("Gary Host") which caused the computer network to identify his computer as "ghost laptop," an apparent reference to its ability to disappear. He also used an email address at mailinator.com that he knew would not be able to be traced to him personally.

On September 25, 2010, using a software program he had specifically designed for the task, Swartz began downloading a massive quantity of academic articles on an automated basis, far more rapidly than he could have done manually, and in a quantity far beyond what any person could actually use for their own academic purposes. This action was contrary to JSTOR's terms of use that users agree to abide by, which do not allow access by automated programs such as web robots, "spiders" and "scrapers." As they became aware of the scope of this automated intrusion, both MIT and JSTOR took steps to terminate Swartz's access through the "ghost computer."

In response, rather than terminating his access, Swartz took specific steps to evade these security responses. On September 26, 2011, Swartz, recognizing that JSTOR had blocked his Internet Protocol ("IP") address, Swartz took steps to obtain a new IP address and immediately reinitiated his program of massive downloading. JSTOR responded by blocking a much broader range of MIT-related IP addresses, in an attempt to shut out the unidentified data thief. MIT also took steps to block access from the "ghost laptop," by

blocking its Media Access Control ("MAC") address, a unique identifier assigned to a network interface. MIT banned the "ghost laptop" from its network for having violated the terms of use that all guests, students and faculty that use MIT's network agree to. These terms include a specific warning that violations may lead to state or federal prosecution.

Nevertheless, on October 2, 2010, Swartz obtained another guest registration by "spoofing" his Acer computer's MAC address, and in so doing obtained a new guest IP address on the MIT network. Again, he used the name "Gary Host," ("ghost laptop"), apparently as a taunt to MIT and JSTOR. On October 8, he connected a second computer to MIT's network. This time he used the name "Grace Host," which the network translated to "ghost macbook." On October 9, 2010, he began using both computers to resume a massive automated downloading of journal articles, causing some of JSTOR's computer servers to shut down as a result of the volume of the demands being placed upon them. As a result of the renewed intrusion, JSTOR blocked access to all MIT users for several days.

In order to obtain an IP address that would not be blocked, Swartz entered a restricted network interface closet in the basement of MIT's Building 16 and physically hard-wired his computer into the MIT network, assigning himself two new IP addresses. The interface closet, known as Room 004T, is controlled by MIT's Information Services and Technology ("IS&T") department. The room was closed at all times and was not even open to members of the MIT community at large, much less individuals who had been forbidden access to MIT's network. In order to avoid his intrusion being discovered, Swartz concealed his computer and a number of external hard drives

underneath a cardboard box in the interface closet, so they would not be readily visible. He continued using the "ghost laptop" to make over two million downloads in November and December of 2010. During the 2010-2011 academic year, MIT had 4,299 undergraduates and 6267 graduate students enrolled. According to MIT records, in November and December, Swartz's downloading represented more than 100 times the total number of downloads made by all other MIT JSTOR users combined. MIT officials detected the laptop and installed a secret camera to identify the intruder.

On January 4, 2011, at approximately 3:26 PM, Swartz entered the room, and appeared to replace a hard drive. He was wearing a dark coat, gray backpack, jeans and a bicycle helmet.

On January 6, 2011, at approximately 12:32 in the afternoon, Swartz again returned to the interface closet, covering his face with a helmet in an apparent effort to evade identification. He took the laptop and hard drive and left the room. MIT Police recognized Swartz riding his bicycle on Lee Street, wearing the same distinctive clothing they had seen on the video feed. When police approached, Swartz leaped off his bike and ran down Lee Street. He was pursued by MIT Police and Secret Service agents, who were able to seize him and arrest him. At the time of his apprehension, Swartz was in possession of a USB drive containing a program, "keepgrabbing2.py," which he had designed to download .pdf files from JSTOR while evading their security countermeasures. When the Acer laptop ("ghost laptop") was recovered and examined forensically pursuant to a search warrant, it proved to contain a software program called "keepgrabbing.py," which served a similar purpose.

In all, Swartz stole more than 4.8 million articles from JSTOR. More than a million of these had been made available for purchase through JSTOR's Publisher Sales Service. The retail price of the files Swartz had illicitly downloaded, had they been purchased from JSTOR, would range into the hundreds of thousands of dollars.

Subsequent to his arrest, Swartz signed an agreement with JSTOR in which he agreed not to further download or disseminate JSTOR's electronic data, nor to "encourage or induce others to harm or interfere with JSTOR computer systems or the computer systems of any of JSTOR's officers, trustees, employee [sic] and other representatives." In exchange, JSTOR agreed not to sue Swartz civilly. The agreement specified that Swartz would pay \$25,000 for JSTOR's legal fees and \$1500 for "nominal damage and loss."

Respectfully Submitted
For the Commonwealth

GERARD T. LEONE, JR.
DISTRICT ATTORNEY

By:

David Marc Solet
Assistant District Attorney
Middlesex District Attorney's Office
15 Commonwealth Avenue
Woburn, MA 01801
Tel: (781) 897-6712
BBO Nos. 652643

Dated: November 2, 2011

Threat Level
Privacy, Crime and Security Online
Previous post
Next post

FBI Investigated Coder for Liberating Paywalled Court Records

By Ryan Singel  October 5, 2009 | 8:48 pm | Categories: Sunshine and Secrecy, The Ridiculous



When 22-year-old programmer Aaron Swartz decided last fall to help an open-government activist amass a public and free copy of millions of federal court records, he did not expect he'd end up with an FBI agent trying to stake out his house.

But that's what happened, as Swartz found out this week when he got his FBI file through a Freedom of Information Act request. A partially-redacted FBI report shows the feds mounted a serious investigation of Swartz for helping put public documents onto the public web.

The FBI ran Swartz through a full range of government databases starting in February, and drove by his home, after the U.S. court system told the feds he'd pilfered approximately 18 million pages of documents worth \$1.5 million dollars. That's how much the public records would have cost through the federal judiciary's pay-walled PACER record system, which charges eight cents a page for most legal filings.

"I think its pretty silly they go after people who use the library to try to get access to public court documents," Swartz said. "It is pretty silly that instead of calling me up, they sent an FBI agent to my house."

The feds also checked Swartz's Facebook page, ran his name against the Department of Labor to figure out his work history, looked for outstanding warrants and prior convictions, checked to see if his mobile phone number had ever come up in a federal wiretap or pen register, and checked him against the records in a private data broker's database.



The Great Court Records Caper began last year when the judiciary and the Government Printing Office experimented with giving away free access to PACER at 17 select libraries around the country. Swartz decided to use the trial to grab as many of the public court records as he could and, perversely, release them to the public.

He visited one of the libraries — the 7th U.S. Circuit Court of Appeals library in Chicago — and installed a small PERL script he'd written. The code cycled sequentially through case numbers, requesting a new document from PACER every three seconds. In this manner, Swartz got nearly 20 million pages of court documents, which his script uploaded to Amazon's EC2 cloud computing service.

Or, as the FBI report put it, the public records were "exfiltrated."

The script ran for a couple of weeks — from September 4 to 22, until the court system's IT department realized something was wrong. Someone was downloading *everything*. None of the records, of course, were private or sealed, and Lexis Nexis has a copy of of PACER's database that it sells a high markup. But Swartz wasn't paying anything.

The Government Printing Office abruptly shut down the free trial and reported to the FBI that PACER was "compromised," the FBI file reveals. The Administrative Office of the U.S. Courts told the FBI in March that Swartz had gained unauthorized access to the free PACER account.

"AARON SWARTZ would have known his access was unauthorized because it was with a password that did not belonged [sic] to him," reads the FBI report summarizing the judiciary's position.

Swartz says his script only ran on the library computer. It didn't use a password at all, but used the PACER authentication cookie set in the PC's browser.

He donated the 19,856,160 pages to public.resource.org, an open government initiative spearheaded by Carl Malamud as part of a broader project to make public as many government databases as Malamud can find. It was Malamud who previously shamed the SEC into putting all its EDGAR filings online in the '90s, and he used \$600,000 in donations to buy 50 years of documents from the nation's appeals court, which he promptly put on the internet for anyone to download in bulk.

The Washington bureau of the FBI opened their investigation of Swartz just a week or so before the *New York Times* published its account of the caper. The bureau didn't contact him then, but in April, the FBI asked to interview the code jock — saying it needed his help to close the "security hole" he'd exploited. When Swartz declined, on the advice of counsel, the feds dropped the investigation after the Justice Department's Computer Crime and Intellectual Property Section closed the case.

Swartz, a former employee of Reddit — a sister company of Wired.com — requested his FBI file in August, and describes it as the "usual mess of confusions that shows the FBI's lack of sense of humor." (Threat Level notes that the FBI's filled Swartz's FOIA request at an admirable speed that would have been unheard of as recently as last year.)

That's how Swartz learned that a Chicago-based FBI agent got Swartz's driver's license photo, and considered a stakeout of his home. But any surveillance, the agent concluded, would be conspicuous, since so few cars were parked on Swartz's dead-end street in Highland Park, Illinois.



The feds evidently identified Swartz in the first place by approaching Amazon, which provided his name, phone number and address. It's not clear if the feds got a subpoena to learn his identity, but they may not have needed one; Amazon's user agreement for its cloud computing solutions gives it the right to turn over customer information to the government on request.

Amazon did not reply to a call and online request for comment.

Two months after opening an investigation, the feds finally called Swartz on April 14. He declined to speak to them, and demurred again through his lawyer two days later.

The investigation was closed on April 20.

PACER records still cost eight cents a page, but now PACER users running the Firefox browser can donate their downloads to the public domain with a simple plug-in called RECAP.

Use of the plug-in is not likely to start an investigation of you.

But then again, who knows.

Photo: Flickr/Creative Commons

See Also:

- [Online Rebel Publishes Millions of Dollars in U.S. Court Records](#)
- [Free the Patents and Laws, Activist Tells Feds](#)
- [Rogue Archivist Campaigns to Be Obama's Printer](#)
- [New Service Makes Tor Anonymized Content Available to All](#)
- [Federal Courts Wary of Document-Sharing Plugin](#)
- [Stars Rise at Startup Summer Camp](#)
- [Firefox Plug-In Frees Court Records, Threatens Judiciary Profits](#)

Tags: aaron swartz, FBI, PACER

[Post Comment](#) | [Permalink](#)

Also on Wired.com

- [Nintendo May Reprint Sold-Out Mario All-Stars](#)
- [Study: Renewable Fuel Mandate Can't Be Met With Ethanol](#)
- [Beans, Soda, Same Difference: A Jelly Belly Experiment](#)
- [Alt Text: Geezerific New Web Services for the Elderly](#)
- [Old School Winter Fun](#)
- [Feds Charge Two for Allegedly Exploiting Bug in Video Poker Machines](#)

Related Topics:



POLICE DEPARTMENT
CAMBRIDGE, MASSACHUSETTS

RECORD OF BOOKING
PLEASE PRINT

CELL NUMBER RELEASED ARREST NUMBER TCAM201100032 DATE & TIME OF BOOKING 01/06/2011 14:46:26 INCIDENT NUMBER 11000131

LAST NAME SWARTZ FIRST AARON MIDDLE NAME H D.O.B. 11/08/1986 AGE 24 SSN (b)(6),(b)(7)(C) (b)(6),(b)(7)(C) 0493

TRUE NAME AARON H SWARTZ MAIDEN NAME HOME PHONE (b)(6),(b)(7)(C)

STREET NO 349 STREET NAME MARSHMAN AVE APT # CITY/TOWN HIGHLAND PARK IL STATE IL ZIP 60035 PHONE (WORK) (CELL)

SEX M HEIGHT 506 WEIGHT 120 RACE WHITE

HAIR BROWN EYES BROWN BLD THIN SKIN FAIR

ETHNICITY NOT OF HISPANIC ORIGIN SCARS LOCATION OF ARREST 24 LEE ST

PLACE OF BIRTH CHICAGO IL MARTIAL STATUS UNMARRIED DRIVER'S LICENSE E2433493 CA

FATHER'S NAME (b)(6),(b)(7)(C) MOTHER'S NAME (b)(6),(b)(7)(C)

EMPLOYER HARVARD U OCCUPATION RESEARCH AT HAR

ADDRESS OF EMPLOYER 124 MOUNT AUBURN ST #52 CAMBRIDGE MA

IF CUT VISIBLE ON PERSON, DESCRIBE KIND & LOCATION no injuries per defendant

TREATED WHERE ATTENDING PHYSICIAN

PRISONER ADVISED OF RIGHTS UNDER G.L. CHAP 276 33A YES BY WHOM (b)(6),(b)(7)(C)

FINGERPRINTS TAKEN YES PHOTO TAKEN YES

IF PRISONER WAS ARRESTED FOR OPERATING UNDER THE INFLUENCE, FILL IN BELOW

PRISONER ADVISED OF RIGHTS UNDER G.L. CHAP 263 5A YES BY WHOM

BREATHLYZER READING BY WHOM

I have been advised of and understand my right to remain silent, use a telephone to call a lawyer or have one provided, and to have my own physician test for alcohol.

PRISONER SIGNATURE ARRESTING OFFICER BOOKING OFFICER

OTHER PD (b)(6),(b)(7)(C) COMPLAINT OTHER PD (b)(6),(b)(7)(C) OFFICER IN CHARGE

IS ARRESTEE A JUVENILE YES

NAME OF PARENT OR GUARDIAN NOTIFIED

RAIL COMMISSIONER (b)(6),(b)(7)(C)

DISPOSITION



OFFENSES

- B&E DAYTIME FOR FELONY c266 S18
- B&E DAYTIME FOR FELONY c266 S18
-
- email ME@AaronSw.com
-

ARREST ON WARRANT? YES WARRANT NUMBER CITY/COURT

CHARGES

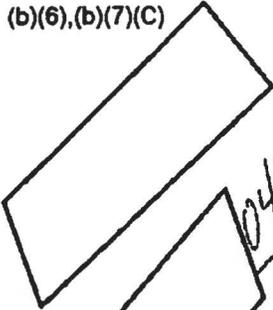
DID ARRESTED PERSON HAVE POSITIVE IDENTIFICATION ID TYPE: STATE ID

NAME OF PROBATION OFFICER NOTIFIED TIME

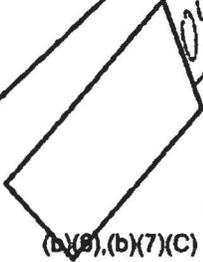
OFFICER MAKING NOTIFICATION TIME

AMOUNT OF BAIL 1,040.00 DATE AND TIME OF BAIL

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



0493



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



Receipt for Transfer of Items

1. Date: 6/27/12		2. Time:	
3. LEO Case #:		4. JIRA #: USSS-148 & 93	
FROM	5. Name: (b)(6),(b)(7)(C)	TO	11. Name: (b)(6),(b)(7)(C)
	6. Title: Forensic LEO /Evidence Tech		12. Title: Special Agent
	7. Agency: CERT/DIID		13. Agency: USSS/Boston
	8. Address: 4500 5 TH Ave, Pittsburgh, PA 15213		14. Address: 10 Causeway St, Suite (b)(6) Boston, MA 02222
	9. Phone #: (b)(6),(b)(7)(C)		15. Phone #: (b)(6),(b)(7)(C) (b)(6),(b)(7)(C)
	10. Signature:		16. Signature:
17. Quantity	18. Description of Item	19. Reason for Transfer	
1	HD 148-1 bc# D01046	Return to Agency	
1	HD 148-2 bc# D01047		
1	HD 148-3 bc# D01048		
1	HD 148-4 D01049		
1	HD 93-3 (148)		
3	Case Files- 144, 93, & 148		

EXTERNAL TRANSFER

DISPATCH DATE: 6/27/2012 SUSPENSE DATE: 6/27/2012

CMU Software Engineering Institute
OLCF8
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
Attn Security Manager

Send to: USSS
10 Causeway St, Suite (b)(6), (b)(7)
Boston, MA 02222

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

ATTENTION: SA (b)(6),(b)(7)(C)

Dispatch Date: 6/27/2012

Sent by: (b)(6),(b)(7)(C)

Suspense Date: 6/27/2012

Document Count: 4

Receipt #: SEIET021

Document Number / Title	Classification	Type	Barcode	Pages
-------------------------	----------------	------	---------	-------

LEOSUPPORTUSSS-148-1 Western Digital, 3.5" 2TB SATA hard drive labeled 102-775-80071, 11m-5014-J6D, 328 containing forensic images	LEO Sensitive	Media	D01048	
---	---------------	-------	--------	--

Control Number: LEOSUPPORTUSSS-148-01

LEOSUPPORTUSSS-148-2 Western Digital, 3.5" 2TB SATA hard drive labeled 102-775-80071, 11m-5014-J6D, 329 containing forensic images	LEO Sensitive	Media	D01047	
---	---------------	-------	--------	--

Control Number: LEOSUPPORTUSSS-148-02

LEOSUPPORTUSSS-148-3 Seagate Barracuda XT, 3.5" 2TB SATA hard drive labeled BOS-102-EVID, 322 image, 321 image	LEO Sensitive	Media	D01048	
---	---------------	-------	--------	--

Control Number: LEOSUPPORTUSSS-148-03

LEOSUPPORTUSSS-148-4 Western Digital, 3.5" 1TB SATA hard drive containing forensic images and labeled "2tbWD in enclos", "Acer", "Harvard iMac", "HP 8GB", "WD1200 from Harv"	LEO Sensitive	Media	D01049	
--	---------------	-------	--------	--

Control Number: LEOSUPPORTUSSS-148-04

Nothing Follows

"I have received the material identified above and assume full responsibility for its safe handling, storage, transmittal elsewhere and/or return in accordance with existing security regulations."

Method: Fed EX

Date Received	Receiver	Signature	Tracking #
6/28/12	(b)(6),(b)(7)(C)	(b)(6),(b)(7)(C)	1Z203VW92460217

Recipient will complete this form, a copy and return original to sender 30 days.

EXTERNAL TRANSFER

DISPATCH DATE: 6/27/2012 SUSPENSE DATE: 6/27/2012

CMU Software Engineering Institute

Send to: USSS

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

10 Causeway St, Suite
Boston, MA 02222

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

4500 Fifth Avenue
Pittsburgh, PA 15213-2812

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

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

ATTENTION:

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

Dispatch Date: 6/27/2012

Sent by:

Suspense Date: 6/27/2012

Document Count: 1

Receipt #: SEIET022

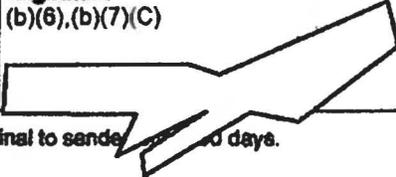
Document Number / Title	Classification	Type	Barcode	Pages
LEO-SUPPORT-USSS-93-3 WD/HD SATA/64MB	LEO Sensitive	Media	D01096	

Control Number:

Nothing Follows

"I have received the material identified above and assume full responsibility for its safe handling, storage, transmittal elsewhere and/or return in accordance with existing security regulations."

Method: Fed EX

Date Received	Receiver	Signature (b)(6),(b)(7)(C)	Tracking #
6/28/12	(b)(6),(b)(7)(C)		1Z203VW9 2460212

Recipient will complete this form, retain a copy and return original to sender within 30 days.

LEO Support - USSS LEOSUPPORTUSSS 93 (b)(6),(b)(7)(C)
Intrusion | BOS | 01/04/2011 Provide support for data acquisition from running system involved in data exfiltration

Details

Type:	Forensics	Status:	Resolved
Priority:	Major	Resolution:	Fixed
Affects Version/s:	None	Fix Versions:	None
Components:	None		
Labels:	None		

Description

Together with SA (b)(6),(b)(7)(C) consulted with SA (b)(6),(b)(7) who was on site at victim institution. Outlined a suggested plan of action that was reviewed and accepted at scene.

Additional data from incident will be sent to dropbox for review and analysis

Activity

- Comments Work Log History Activity
- (b)(6),(b)(7)(C) added a comment - 04/Jan/11 5:50 PM
- SA (b)(6),(b)(7) reviewing initial batch of data uploaded to dropbox
- (b)(6),(b)(7)(C) added a comment - 28/Jan/11 12:21 PM
- No further action required.
- (b)(6),(b)(7)(C) added a comment - 28/Jan/11 12:22 PM
- Offender arrested. No further action required.
- (b)(6),(b)(7)(C) added a comment - 02/Feb/11 5:30 PM - Restricted to leo-support-uss
- Analysis of network traffic from incident is requested. Approximately 80 GB of data will be FEDEX'd to CERT.

The AUSA requests the following information Per EOUSA

(b)(5)

- (b)(6),(b)(7)(C) added a comment - 16/Feb/11 12:17 PM - Restricted to leo-support-uss - edited
- (b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) have performed analysis of the PCAP files submitted and provided a summary of the contents via email to the USSS case agent.

(b)(6),(b)(7)(C) added a comment - 28/Feb/11 2:45 PM - Restricted to leo-support-uss
Case material subject to grand jury non-disclosure requirements (b)(6),(b)(7) and (b)(6),(b)(7)(C) added to
6e list for material.

(b)(6),(b)(7)(C) added a comment - 31/Mar/11 11:03 AM - Restricted to leo-support-uss
(b)(6),(b)(7)(C) and (b)(6),(b)(7)(C) met with AUSA Stephen Heymann on Friday, Mar 25. Confirmed that analysis
supplied so far has met case requirements, answered additional questions, discussed subsequent decision
points for the prosecution.

Will consult with SA (b)(6),(b)(7)(C) to determine if request can be closed and whether related requests will be
assigned new tracking entries.

(b)(6),(b)(7)(C) added a comment - 07/Apr/11 10:49 AM - Restricted to leo-support-uss
(b)(6),(b)(7)(C) submitted requested analysis of Python programs and bash history, correlating with other data
and evidence in the case. Findings discussed with AUSA Stephen Heymann.

(b)(6),(b)(7)(C) added a comment - 07/Apr/11 10:51 AM - Restricted to leo-support-uss
Marking resolved -- but pre-trial assistance may be needed.

(b)(6),(b)(7)(C) added a comment - 27/Jul/11 3:42 PM - Restricted to leo-support-uss - edited
(b)(6),(b)(7)(C) and (b)(6) had further discussion with AUSA Stephen Heymann on 7/26 regarding clarification of
previously provided analysis assistance findings
Further discussions may be necessary as the matter progresses.

At this point, no further assistance is requested, however.

People

Assignee: (b)(6),(b)(7)(C)
Reporter:
Vote (0)

Dates

Created: 04/Jan/11 5:50 PM
Updated: 27/Jul/11 3:42 PM
Resolved: 07/Apr/11 10:51 AM

6/24/2012 10:16 PM



DEPARTMENT OF HOMELAND SECURITY
UNITED STATES SECRET SERVICE
10 Causeway St, Suite 447 Boston, MA 02222

MEMORANDUM

DATE: Friday, March 28, 2014

FROM: (b)(6) (b)(7)(C)
Special Agent
US Secret Service
Boston Field Office

SUBJECT: Preservation Order

Our agency is conducting an ongoing criminal investigation that involves one or more account holders. As part of that investigation, we are requesting that information related to all email accounts associated with @aaronsw.com be preserved pending the issuance of formal legal process. More specifically, we are requesting that you preserve all subscriber information and/or account contents or group information related to the customer or subscribers. Additionally we are asking that all private messages, correspondence and bulletin board postings from above named users be preserved. We are also asking that all web content be preserved.

At this time we are expecting to obtain formal legal process in the next 90 days. We acknowledge that if we do not serve legal process upon you in the next 90 days, and do not request a 90 day extension, the preserved information may no longer be available.

Point of contact for this request is SA (b)(6) (b)(7)(C) at (b)(6) (b)(7)(C) or (b)(6) (b)(7)(C) @usss.dhs.gov

(b)(6) (b)(7)(C)
Special Agent
US Secret Service

Friday, March 28, 2014

GMail, Google Inc.
Subpoena Compliance Department
Attn: (b)(6) (b)(7)(C)
1600 Amphitheater Parkway
Mountain View CA 94043
FAX # (650) 649-2939

Dear Custodian of Records:

Our agency is conducting an ongoing criminal investigation that involves one or more account holders. As part of that investigation, we are requesting that information related to all email accounts associated with @aaronsw.com be preserved pending the issuance of formal legal process. More specifically, we are requesting that you preserve all subscriber information and/or account contents or group information related to the customer or subscribers. Additionally we are asking that all private messages, correspondence and bulletin board postings from above named users be preserved. We are also asking that all web content be preserved .

At this time we are expecting to obtain formal legal process in the next 90 days. We acknowledge that if we do not serve legal process upon you in the next 90 days, and do not request a 90 day extension, the preserved information may no longer be available.

Point of contact for this request is SA (b)(6) (b)(7)(C) at (b)(6) (b)(7)(C) or (b)(6) (b)(7)(C) @uss.s.dhs.gov

Respectfully

(b)(6) (b)(7)(C)
Special Agent
United States Secret Service
10 Causeway Street.
Suite 447
Boston, MA. 02222



M.I.T. POLICE
301 VASSAR ST CAMBRIDGE, MA

COPY

INCIDENT # / REPORT # 11000351 / 1
OFFICER (b)(6), (b)(7)(C)
RANK DETECTIVE
REVIEW STATUS APPROVED BY (b)(6), (b)(7)(C)

Not For Public Release Date/Time Printed: Fri Feb 25 14:20:29 EST 2011 By (b)(6), (b)(7)(C)

INCIDENT #11000351 DATA
As Of 01/25/2011 08:55:10

BASIC INFORMATION

CASE TITLE B&E
LOCATION 21 AMES ST
APT/UNIT
CITY, STATE CAMBRIDGE, MA

DATE/TIME REPORTED 01/06/2011 14:20:45
DATE/TIME OCCURRED On or after 01/04/2011 15:26

INCIDENT TYPE/OFFENSE
B&E DAYTIME FOR FELONY c266 S18

PERSONS

ROLE	NAME	SEX	RACE	AGE	DOB	PHONE
VICTIM	MIT, ADDRESS: 77 MASSACHUSETTS AVE CAMBRIDGE, MA					(HOME) (CELL)
WITNESS	(b)(6), (b)(7)(C) ADDRESS: (b)(6), (b)(7)(C)	MALE	(b)(6), (b)(7)(C)	08/03/1990		(HOME) (CELL) (b)(6), (b)(7)

OFFENDERS

STATUS	NAME	SEX	RACE	AGE	DOB	PHONE
DEPNDANT	SWARTZ, AARON H ADDRESS: , IL	MALE	UNKNOWN	24	11/08/1986	(HOME) (CELL)

[NO VEHICLES]

PROPERTY

CLASS	DESCRIPTION	MAKE	MODEL	SERIAL #	VALUE
-------	-------------	------	-------	----------	-------

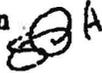
OFFICER REPORT: 11000351 - 1 / (b)(6), (b)(7)(C)

DATE/TIME OF REPORT	TYPE OF REPORT	REVIEW STATUS
01/06/2011 14:20:45	INCIDENT	APPROVED

Memorandum

United States Attorney
District of Massachusetts



Subject Re: Filter Team Instructions Concerning Search of IMac Model A1311, Serial number WB025AXGD87, Western Digital Hard Drive Model WD1200, Serial number WMANN1006724 and Sony Micro Vault USB Drive marked SDK USM 8GH(B)	Date February 18, 2011
To AUSA (b)(6),(b)(7)(C) Special Agent (b)(6),(b)(7)(C) Forensic Agents	From AUSA Stephen P. Heymann 

As we understand it, Aaron Swartz retained attorney Philip Cormier on January 6, 2011, following his arrest for breaking and entering at MIT. As a consequence, it is possible that communications between Swartz and Cormier, the law firm Good and Cormier, or Cormier's partner, Andrew Good, may be stored on the iMac computer, the Western Digital hard drive, and/or the Sony USB drive which we seized pursuant to search warrants on February 11, 2011. To minimize the chance that members of the investigative team will be exposed to attorney/client communications pertaining to that state case, we are implementing the following filtering protocol. AUSA (b)(6),(b)(7)(C) who is otherwise not involved in any manner with the investigation will be available to answer any questions. His telephone number is (b)(6),(b)(7)(C)

Forensic agents not otherwise involved in any aspect of the main investigation will conduct an initial review of the seized iMac, Western Digital hard drive and USB drive. It will be their task to identify and filter-out any attorney/client communications to the fullest extent

Page 2

practicable. Towards this end, the filter team will conduct an initial search of the computer and two drives for the following terms:

goodcornier
agood
pcornier
Andrew Good
Mr. Good

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

Andrew
Philip Cornier
Mr. Cornier

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

Philip

The filter team will then examine each of the documents, records and e-mails ("the objects") containing one of these terms only to the extent necessary to establish if it contains an attorney/client communication. If the object does, the filter team will determine the object's hash value and add the hash value to a filter set. Agents involved with the investigation will use this hash set to filter out objects containing attorney/client communications prior to their search, examination and analysis of the computer and drives.

The hash value set should be preserved, should it be needed at a later point in the case.

Attachment A

You are required to produce the following objects:

All computers, hard drives, USB drives, DVDs, CDs and other electronic and optical storage devices currently or previously owned or possessed by Aaron Swartz at any time from September 1, 2010 to the present. These shall include, without limitation, all computers and hard drives transferred to you by Aaron Swartz, loaned by you to Aaron Swartz, loaned to you by Aaron Swartz, or stored by or on behalf of Aaron Swartz at any premises over which you have custody or control. These shall also include all files, documents, records and data stored on such devices.

You are required to produce all documents, records and data relating to, regarding or referring to the following:

• JSTOR, including, without limitation,

- (1) Jstor.org;
- (2) Journals documents, records and data digitized by JSTOR,
- (3) Journals, documents, records and data stored by JSTOR;
- (4) Journals, documents, records and data originating at JSTOR;
- (5) Means of access to JSTOR;
- (6) Computer software capable of making repeated requests for documents, records and data from JSTOR;

*@ 2:25 PM
4/13/11
S. Heyman
Reviews list*



- (7) Computer software capable of making repeated downloads of documents, records and data from JSTOR.
- Massachusetts Institute of Technology, including, without limitation,
 - (1) Mit.edu;
 - (2) IP addresses in the class A domain 18;
 - (3) MIT's computer network;
 - (4) MIT's physical plant.
 - Remote electronic storage locations of more than 100 .pdf files.
 - Modifying and modified MAC addresses.
 - Electronic communications with Aaron Swartz between September 1, 2010 and January 15, 2011.
 - Electronic downloading, transfer and storage of journal articles, including, without limitation, all communications with Aaron Swartz with respect to this subject matter.
 - Concealment or storage of computers or hard drives.
 - Arrests, searches, criminal investigations or prosecutions, actual or anticipated, of Aaron Swartz, his residence or office between January 6 - 15, 2011, including, without limitation, all communications with Aaron Swartz concerning this subject matter.

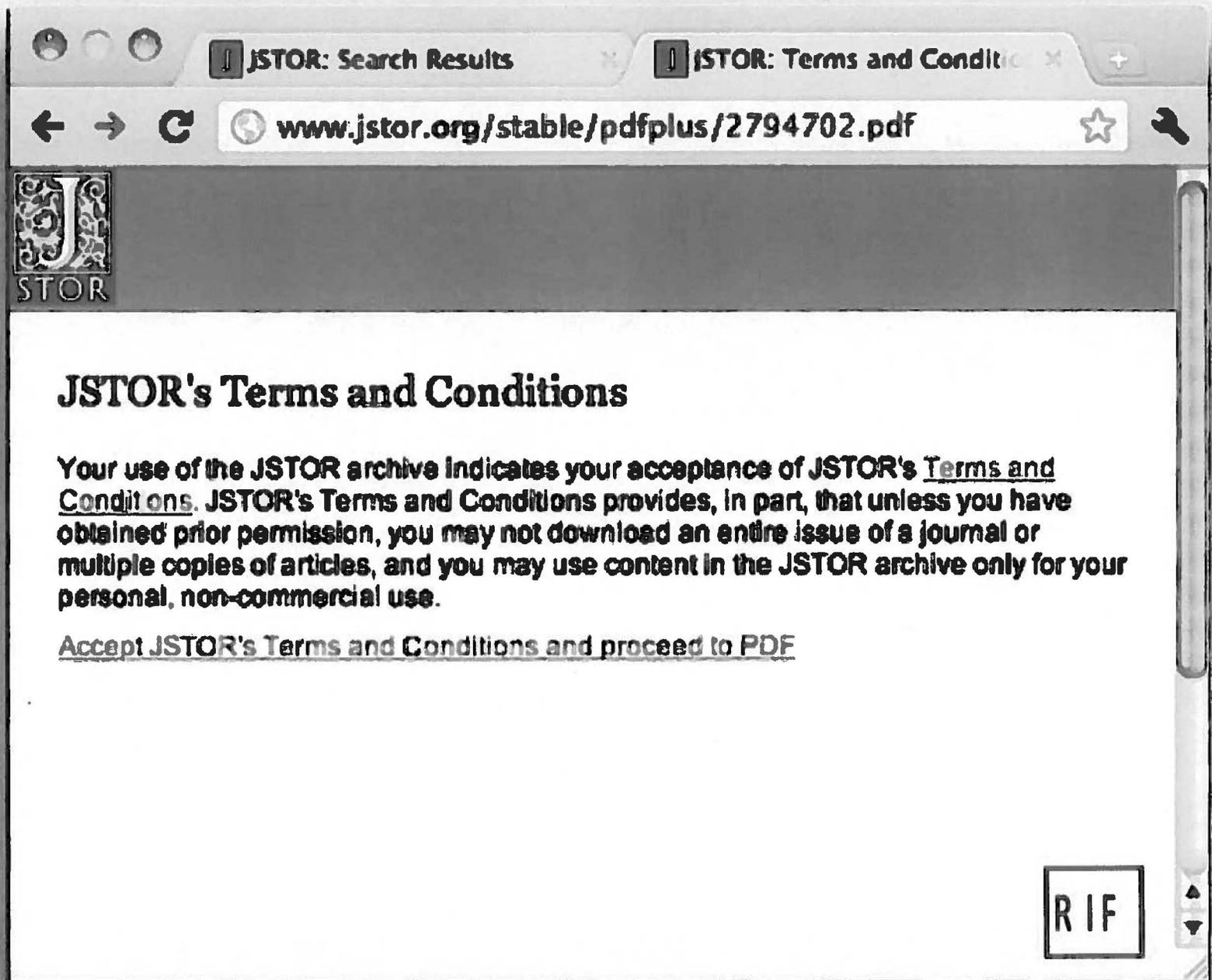
For the purpose of this subpoena, "documents, records and data" include, without limitation, all written, printed, typed, photographed, recorded or otherwise reproduced or stored communications or representations, whether comprised of letters, words, numbers, pictures,

sounds or symbols, or any combination thereof, whether deliberately, inadvertently or automatically stored. "Documents, records and data" include copies or duplicates of documents contemporaneously or subsequently created which have any non-conforming notes or other markings and the backsides of any communications or representations which contain any of the above, and all deleted files and e-mails which are available from system back-ups.

By way of example, "documents, records and data" include, but are not limited to: electronic mail; instant messages; computer files; correspondence; memoranda; notebooks; notes; drafts; records; letters; envelopes; telegrams; messages; descriptions; plans; schematics; diagrams; drawings; specifications; analyses; agreements; accounts; checks; bank statements; payroll records; contracts; employment agreements; working papers; reports and summaries of investigations; trade letters; press releases; comparisons; books; notices; drawings; diagrams; instructions; manuals; calendars; diaries; articles; magazines; newspapers; brochures; guidelines; notes or minutes of meetings or of other communications of any type, including inter- and intra-office or company communications; questionnaires; surveys; charts; graphs; photographs; files or videos; tapes; discs; data cells; bulletins; printouts of information stored, maintained, or transmitted by electronic data or word processing equipment; electronic claims filing and transmittals; invoices; and all other data compilations from which this information can be obtained including optical and electromagnetically sensitive stored media.

Please provide all documents, records, data, files and logs electronically.





JSTOR's Terms and Conditions

Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions. JSTOR's Terms and Conditions provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use.

[Accept JSTOR's Terms and Conditions and proceed to PDF](#)



The image shows a screenshot of a web browser window. At the top, there are two tabs: "JSTOR: Search Results" and "JSTOR: Terms and Conditions". The address bar contains the URL "www.jstor.org/stable/pdfplus/2794702.pdf". The JSTOR logo is visible in the top left corner of the page content. The main heading is "JSTOR's Terms and Conditions". Below the heading, a paragraph states: "Your use of the JSTOR archive indicates your acceptance of JSTOR's Terms and Conditions. JSTOR's Terms and Conditions provides, in part, that unless you have obtained prior permission, you may not download an entire issue of a journal or multiple copies of articles, and you may use content in the JSTOR archive only for your personal, non-commercial use." Below this paragraph is a link that says "Proceed to PDF". In the bottom right corner of the page content, there is a small box containing the letters "R I F".

The liberal dissemination of knowledge is essential to scientific inquiry, more than in any other area. The application of scientific methods to the study of human behavior is no exception. The publication of scientific papers is a public good, and the authors are already being paid for their work. The only way to ensure that the scientific record is preserved is to make it available to all. Our continued survival may even depend on it.

If I can remove even one pillar of ill-considered laws from a politician's library, then I can remove scientific and historic understanding from whatever political class I suffer will be justified. It will be one less dollar spent in the war against knowledge. Our laws shall open a crack.

I had considered releasing this collection anonymously, but others pointed out that the copyright proprietors of many books would probably access this and add it to their growing list of violations. I have decided to release this collection under a Creative Commons license that prohibits such usage. I sincerely believe that applying such usage to such attaching post cards is

I'm interested in hearing about any enjoyable discoveries or even useful applications which come of this archive

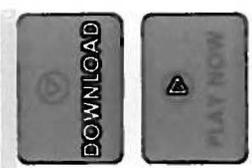
```
-----
File: [redacted]
Version: 0.0.1
URL: [redacted]
-----
```

DOWNLOAD THIS TORRENT (MAGNET LINK)

Comments

- 11-07-21 09:25 CET:**
Unfortunately this torrent file was created with a rather poor selection of trackers and private key won't let me change it or update another version.
- 11-07-21 14:09 CET:**
If it's not working well for you, try the torrent at <http://www.bittor.com/torrents/18729> which is the same system but it just has more seeders/trackers.
- 11-07-21 14:09 CET:**
Can someone update this to work and Archiving to make every single entry easy to find for researchers like people?
- 11-07-21 14:09 CET:**
There are the address of a home, I am so sending this.
- 11-07-21 14:09 CET:**
bittor: From the scientific data! There is finally no legitimate reason to keep things so old like those behind a paywall!
- 11-07-21 14:16 CET:**
bittor: I'm not sure if you want to create your torrent as a private torrent making it necessary to use just any kind of tracker address.
- 11-07-21 14:16 CET:**
If your torrent is not private but public, then bittor software will also use decentralized means to find and share files, also like networks and not just tracker network.
- 11-07-21 14:16 CET:**
So how did you create your torrent?
recreate the torrent as public if you have made a mistake on the first place and re-share it.
- 11-07-21 14:16 CET:**
works!

bittor.com says your torrent is not private, so no big deal, torrent clients will find other peers themselves even with just a single tracker or all bittor clients.



[torrentcreator.com](#) says you should create your torrent as a private torrent making it necessary to use just any kind of tracker address.

if your torrent is not private but public, then torrent software will also use decentralized means to find and share files, also this means it will not just track it.

so how did you create your torrent?

recreate the torrent as public if you have made a mistake in the first place and re-share it.

simple as that.

[torrentcreator.com](#) says your torrent is not private, so no big deal, torrent clients will find other peers themselves even with just a single tracker or all being offline.

you can manually add more and more trackers as they wish, but it all doesn't matter at all.

decentralized tracking is available already, you have created your torrent properly to make it as a public torrent.

never create private torrents, that doesn't make any sense at all in terms of uptime and availability.

Oh, well try to update this to archlinux and BSD to make it easy to find using google. Right like some people to do so with my other home connection and using TOR (don't want to get used by the software for sharing files).

The church of bitcoin issued a presser <http://www.bitcoin.org/2011/07/21/a-distributed-network-for-the-world/>

Mr. Harvard, I applaud you.

I have often myself run into the very walls of BTOR, Bittor, Bittor and the like (most universities can not afford to subscribe to all journals).

I am therefore well acquainted with the frustration of having access made progressively inaccessible to me - especially that in many instances first paid by society and then later capped to increase the profits of the few.

I sincerely hope that your actions, as well as those of Aaron Swartz herald the beginning of the end for the BigBrother business of exorbitant access prohibitions.

I don't know if this is a problem only to me, but encoding leaves behind the BOP signatures.

In case other people are not being able to verify the signatures, I found the encoding in a way that the signature is valid, and copied it here:

<http://pastebin.com/7uqf8f8y>

You, sir, are a hero.

Thank you.

Sure you are a hero.

[Logon](#) | [Register](#) | [Language / Select language](#) | [About](#) | [Legal](#) | [Terms](#) | [Blog](#)

[Contact us](#) | [Privacy policy](#) | [Downloads](#) | [Doodles](#) | [Search](#) | [Cloud](#) | [Top Cloud](#) | [Forum](#) | [TPO](#) | [T-shirts](#)

[Signatures](#) | [Signatures](#)

3,089,311 registered users. Last updated 10/26/10.

75,040,507 users (27,975,277 readers - 47,065,230 teachers) in 2,378,781 torrents.

